Service Manual

hp StorageWorks Edge Switch 2/32

Product Version: FW v06.xx/HAFM SW v08.02.00

Third Edition (July 2004)

Part Number: AA-RS2GD-TE

This manual describes diagnostic procedures, repair procedures, and the removal and replacement procedures for Field-Replaceable Units (FRUs) for the HP StorageWorks Edge Switch 2/32.

Edge Switch 2/32 Service Manual
Third Edition (July 2004)
Part Number: AA-RS2GD-TE

contents

Figures

Tables

About This Guide

This service manual provides information to help you:

- Monitor and troubleshoot the Edge Switch 2/32.
- Perform procedures to isolate and resolve problems.
- Remove and replace Field Replaceable Units (FRUs).

"About this Guide" topics include:

Overview

This section covers the following topics:

Intended Audience

This book is intended for use by service technicians who are experienced with the following:

- Fibre Channel technology.
- StorageWorks Fibre Channel switches by Hewlett-Packard.

Related Documentation

For a list of corresponding documentation included with this product, see the Related Documents section of the HP StorageWorks Release Notes.

For the latest information, documentation, and firmware releases, please visit the HP StorageWorks web site:

http://h18006.www1.hp.com/storage/saninfrastructure.html

For information about Fibre Channel standards, visit the Fibre Channel Industry Association web site, located at http://www.fibrechannel.org

Conventions

Conventions consist of the following:

- Document Conventions
- Text Symbols
- Equipment Symbols

Document Conventions

This document follows the conventions in Table 1.

Table 1: Document conventions

Convention	Element
Blue text: Figure 1	Cross-reference links
Bold	Menu items, buttons, and key, tab, and box names
Italics	Text emphasis and document titles in body text
`Monospace font`	User input, commands, code, file and directory names, and system responses (output and messages)
`Monospace, italic font`	Command-line and code variables
Blue underlined sans serif font text (http://www.hp.com)	Web site addresses

Text Symbols

The following symbols may be found in the text of this guide. They have the following meanings:

WARNING: Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or death.

Caution: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or data.

Tip: Text in a tip provides additional help to readers by providing nonessential or optional techniques, procedures, or shortcuts.

Note: Text set off in this manner presents commentary, sidelights, or interesting points of information.

Equipment Symbols

The following equipment symbols may be found on hardware for which this guide pertains. They have the following meanings:

Any enclosed surface or area of the equipment marked with these symbols indicates the presence of electrical shock hazards. Enclosed area contains no operator serviceable parts.

WARNING: To reduce the risk of personal injury from electrical shock hazards, do not open this enclosure.

Any RJ-45 receptacle marked with these symbols indicates a network interface connection.

WARNING: To reduce the risk of electrical shock, fire, or damage to the equipment, do not plug telephone or telecommunications connectors into this receptacle.

Any surface or area of the equipment marked with these symbols indicates the presence of a hot surface or hot component. Contact with this surface could result in injury.

WARNING: To reduce the risk of personal injury from a hot component, allow the surface to cool before touching.

Power supplies or systems marked with these symbols indicate the presence of multiple sources of power.

WARNING: To reduce the risk of personal injury from electrical shock, remove all power cords to completely disconnect power from the power supplies and systems.

Any product or assembly marked with these symbols indicates that the component exceeds the recommended weight for one individual to handle safely.

WARNING: To reduce the risk of personal injury or damage to the equipment, observe local occupational health and safety requirements and guidelines for manually handling material.

Rack Stability

Rack stability protects personnel and equipment.

WARNING: To reduce the risk of personal injury or damage to the equipment, be sure that:

- The leveling jacks are extended to the floor.
- The full weight of the rack rests on the leveling jacks.
- In single rack installations, the stabilizing feet are attached to the rack.
- In multiple rack installations, the racks are coupled.
- Only one rack component is extended at any time. A rack may become unstable if more than one rack component is extended for any reason.

Getting Help

If you still have a question after reading this guide, contact an HP authorized service provider or access our web site: http://www.hp.com.

HP Technical Support

Telephone numbers for worldwide technical support are listed on the following HP web site: http://www.hp.com/support/. From this web site, select the country of origin.

Note: For continuous quality improvement, calls may be recorded or monitored.

Be sure to have the following information available before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

HP Storage Web Site

The HP web site has the latest information on this product, as well as the latest drivers. Access storage at: http://www.hp.com/country/us/eng/prodserv/storage.html. From this web site, select the appropriate product or solution.

HP Authorized Reseller

For the name of your nearest HP authorized reseller:

- In the United States, call 1-800-345-1518
- In Canada, call 1-800-263-5868
- Elsewhere, see the HP web site for locations and telephone numbers: http://www.hp.com.

General Information

1

The HP StorageWorks Edge Switch 2/32 provides dynamic switched connections between Fibre Channel servers and devices in a storage area network (SAN) environment. SANs introduce the concept of server-to-device networking and multi-switch fabrics, eliminate requirements for dedicated connections, and enable the enterprise to become data centric.

A SAN provides speed, high capacity, and flexibility for the enterprise, and is primarily based upon Fibre Channel architecture. The switch implements Fibre Channel technology that provides a bandwidth of 2.125 gigabits per second, redundant switched data paths, a scalable number of active ports, and long transmission distances (up to 35 kilometers).

Switch Description

The Edge Switch 2/32 provides Fibre Channel connectivity through 32 generic mixed ports (GX_Ports). Switch ports operate at either 1.0625 or 2.125 gigabits per second (Gb/s), and can be configured as:

- Fabric ports (F_Ports) to provide direct connectivity for up to 32 switched fabric devices.
- Fabric loop ports (FL_Ports) to provide arbitrated loop connectivity and fabric attachment for FC-AL devices. Each FL_Port can theoretically support the connection of 126 FC-AL devices.
- Expansion ports (E_Ports) to proved interswitch link (ISL) connectivity to fabric directors and switches.

The switch can be installed on a table or desk top, or mounted in an equipment cabinet, or in any standard equipment rack.

The switch provides dynamic switched connections for servers and devices, supports mainframe and open-systems interconnection (OSI) computing environments, and provides data transmission and flow control between device node ports (N_Ports) as specified by the Fibre Channel Physical and Signaling Interface (FC-PH 4.3). Through ISLs, the switch can connect additional switches to form a Fibre Channel multi-switch fabric.

The Edge Switch 2/32 provides connectivity for devices manufactured by multiple original equipment manufacturers (OEMs). To determine if an OEM product can communicate through connections provided by the switch, or if communication restrictions apply, refer to the supporting publications for the product or contact your HP marketing representative.

Maintenance Approach

Whenever possible, the maintenance approach instructs service personnel to perform fault isolation and repair procedures without degrading or interrupting operation of the switch, attached devices, or associated applications.

Switch fault isolation begins when one or more of the following occur:

- System event information displays at the attached HAFM appliance, a remote workstation communicating with the HAFM appliance, or the Embedded Web Server (EWS) interface.
- LEDs on the switch front panel or FRUs illuminate to indicate a hardware malfunction.
- An unsolicited SNMP trap message is received at a management workstation, indicating an operational state change or failure.
- Notification of a significant system event is received at a designated support center through an e-mail message or the call-home feature.

System events can be related to one of the following:

- Switch or HAFM appliance failure (hardware or software).
- Ethernet LAN communication failure between the switch and HAFM appliance.
- Link failure between a port and attached device.
- ISL failure or segmentation of an E_Port.

Fault isolation and service procedures vary depending on the system event information provided. Fault isolation and related service information are provided through maintenance analysis procedures (MAPs) documented in Chapter 3. MAPs consist of step-by-step procedures that prompt service personnel for information or describe a specific action to be performed.

MAPs provide information to interpret system event information, isolate a switch failure to a single FRU, remove and replace the failed FRU, and verify switch operation. The fault isolation process normally begins with “MAP 0000: Start MAP” on page 29.

Before using these procedures, ensure the correct switch is selected for service (if the HAFM appliance manages multiple switches or other High Availability Fabric Directors and Edge Switches) by enabling unit beaconing at the failed switch. The amber system error LED on the switch front panel blinks when beaconing is enabled. Instructions to enable beaconing are incorporated into MAP steps.

Tools and Test Equipment

This section describes tools and test equipment that may be required to install, test, service, and verify operation of the switch and attached HAFM appliance.

Tools Supplied with the Switch

Tools are supplied with the switch or must be supplied by service personnel. Use of the tools may be required to perform one or more installation, test, service, or verification tasks.

- **Fiber-optic loopback plug–**An SFP multimode (shortwave laser) or singlemode (longwave laser) loopback plug is required to perform port loopback diagnostic tests. One loopback plug is shipped with the switch, depending on the type of port transceivers installed. Both plugs are shipped if shortwave laser and longwave laser transceivers are installed. The plug is shown in Figure 1.

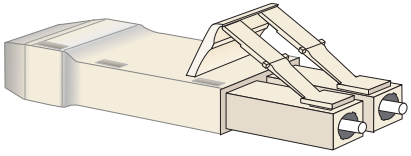


Figure 1: Multimode and singlemode loopback plugs

- **Fiber-optic protective plug–**For safety and port transceiver protection, fiber-optic protective plugs must be inserted in all port SFPs without fiber-optic cables attached. The switch is shipped with protective plugs installed in all ports. A protective plug is shown in Figure 2.

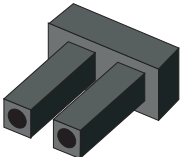


Figure 2: Fiber-optic protective plug

- **Null modem cable–**An asynchronous RS-232 null modem cable is required to configure switch network addresses and acquire Event Log information through the maintenance port. The cable has nine conductors and DB-9 male and female connectors. A null modem cable is not a standard (straight-through) RS-232 cable. Refer to Figure 3.

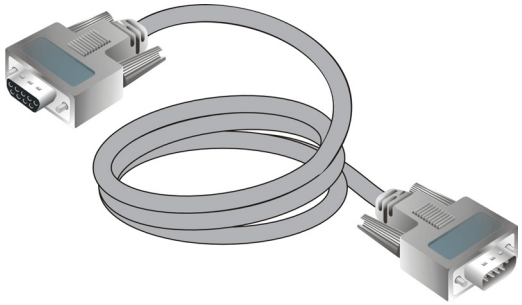


Figure 3: Null modem cable

Tools Supplied by Service Personnel

The following tools are expected to be supplied by service personnel performing switch installation and maintenance actions. Use of the tools may be required to perform one or more installation, test, service, or verification tasks.

- **Scissors or pocket knife–**A sharp cutting edge (scissors or knife blade) may be required to cut the protective strapping when unpacking the switch, HAFM appliance, Ethernet hub, or replacement FRUs.
- **Standard flat-tip and cross-tip (Phillips) screwdrivers–**Screwdrivers are required to remove, replace, adjust, or tighten various connector or chassis components, and to remove and replace power supplies.
- **Maintenance terminal (desktop or notebook PC)–**The PC is required to configure switch network addresses and acquire Event Log information through the maintenance port.

  The PC must have:

  — The Microsoft® Windows® 98, Windows 2000, or Windows Millennium Edition operating system installed.

  — RS-232 serial communication software (such as *ProComm Plus*™ or *HyperTerminal*) installed. *HyperTerminal* is provided with Windows operating systems.
- **Fiber-optic cleaning kit–**The kit contains tools and instructions to clean fiber-optic cable, connectors, loopback plugs, and protective plugs.

Additional Information

The following Edge Switch 2/32 documents provide additional information:

- For detailed information about Edge Switch 2/32 front and rear panel features, field replaceable units (FRUs), management options and operational features, installation, configuration and technical specifications, see the *HP StorageWorks Edge Switch 2/32 Installation Guide*.
- For information on managing the Edge Switch 2/32 using the *High Availability Fabric Manager* (*HAFM*) and *Element Manager* applications, see the *HP StorageWorks Edge Switch Element Manager User Guide.*

Diagnostics

2

This chapter describes diagnostic procedures used by service representatives to isolate HP StorageWorks Edge Switch 2/32 problems or failures to the field-replaceable unit (FRU) level. The chapter specifically describes how to perform maintenance analysis procedures (MAPs).

Maintenance Analysis Procedures

Maintenance Analysis Procedures (MAPs) provide fault isolation and related service procedures. They are step-by-step procedures that prompt service personnel for information and describe a maintenance action. They provide information to interpret system events, isolate a switch failure to a single FRU, remove and replace the failed FRU, and verify switch operation.

Factory Defaults

Table 2 lists the defaults for the passwords, and IP, subnet, and gateway addresses.

Table 2: Factory-Set Defaults

Item	Default
Customer password	password
Maintenance password	level-2
IP address	10.1.1.10
Subnet mask	255.0.0.0
Gateway address	0.0.0.0

Quick Start

Table 3 lists and summarizes the MAPs. Fault isolation normally begins at "MAP 0000: Start MAP" on page 29.

Table 3: MAP Summary

MAP	Page
MAP 0000: Start MAP	page 29
MAP 0100: Power Distribution Analysis	page 51
MAP 0200: POST Failure Analysis	page 59
MAP 0300: HAFM Appliance Software Problem Determination	page 61
MAP 0400: Loss of HAFM Appliance or Web Browser PC Communication	page 69
MAP 0500: FRU Failure Analysis	page 83
MAP 0600: Port Failure and Link Incident Analysis	page 89
MAP 0700: Fabric, ISL, and Segmented Port Problem Determination	page 107
MAP 0800: HAFM Appliance or Web Browser PC Hardware Problem Determination	page 122

Table 4 lists event codes and the corresponding MAP references. The table provides a quick start guide if an event code is readily available.

Table 4: Event Codes versus Maintenance Action

Event Code	Explanation	Action
011	Login Server database invalid.	Go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination.
021	Name Server database invalid.	Go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination.
031	SNMP request received from unauthorized community.	Add a community name through the *Element Manager* application.
051	Management Server database invalid.	Go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination.

Table 4: Event Codes versus Maintenance Action (Continued)

Event Code	Explanation	Action
052	Management Server internal error.	Go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination.
061	Fabric Controller database invalid.	Go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination.
062	Maximum interswitch hop count exceeded.	Go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination.
063	Remote switch has too many ISLs.	Go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination.
070	E_Port is segmented.	Go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination.
071	Switch is isolated.	Go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination.
072	E_Port connected to unsupported switch.	Go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination.
073	Fabric initialization error.	Go to "Collecting Maintenance Data" on page 151.
074	ILS frame delivery error threshold exceeded.	Go to "Collecting Maintenance Data" on page 151.
080	Unauthorized worldwide name.	Go to MAP 0600: Port Failure and Link Incident Analysis.
081	Invalid attachment.	Go to MAP 0600: Port Failure and Link Incident Analysis
120	Error detected while processing system management command.	Go to "Collecting Maintenance Data" on page 151.
121	Zone set activation failed–zone set too large.	Reduce size of zone set and retry.

Table 4: Event Codes versus Maintenance Action (Continued)

Event Code	Explanation	Action
140	Congestion detected on an ISL.	Go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination.
141	Congestion relieved on an ISL.	No action required.
142	Low BB_Credit detected on an ISL.	Go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination.
143	Low BB_Credit relieved on an ISL.	No action required.
150	Zone merge failure.	Go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination.
151	Fabric configuration failure.	Go to "Collecting Maintenance Data" on page 151.
200	Power supply AC voltage failure.	Go to MAP 0100: Power Distribution Analysis.
201	Power supply DC voltage failure.	Go to MAP 0100: Power Distribution Analysis.
203	Power supply AC voltage recovery.	No action required.
204	Power supply DC voltage recovery.	No action required.
206	Power supply removed.	Replace FRU.
207	Power supply installed.	No action required.
300	Cooling fan propeller failed.	Go to MAP 0500: FRU Failure Analysis.
301	Cooling fan propeller failed.	Go to MAP 0500: FRU Failure Analysis.
302	Cooling fan propeller failed.	Go to MAP 0500: FRU Failure Analysis.
303	Cooling fan propeller failed.	Go to MAP 0500: FRU Failure Analysis.
304	Cooling fan propeller failed.	Go to MAP 0500: FRU Failure Analysis.
305	Cooling fan propeller failed.	Go to MAP 0500: FRU Failure Analysis.

Table 4: Event Codes versus Maintenance Action (Continued)

Event Code	Explanation	Action
310	Cooling fan propeller recovered.	No action required.
311	Cooling fan propeller recovered.	No action required.
312	Cooling fan propeller recovered.	No action required.
313	Cooling fan propeller recovered.	No action required.
314	Cooling fan propeller recovered.	No action required.
315	Cooling fan propeller recovered.	No action required.
400	Power-up diagnostic failure.	Go to MAP 0200: POST Failure Analysis.
410	Switch reset.	No action required.
411	Firmware fault.	Go to MAP 0200: POST Failure Analysis.
412	CTP watchdog timer reset.	Go to "Collecting Maintenance Data" on page 151.
421	Firmware download complete.	No action required.
423	CTP firmware download initiated.	No action required.
426	Multiple ECC single-bit errors occurred.	Go to MAP 0500: FRU Failure Analysis.
433	Non-recoverable Ethernet fault.	Go to MAP 0500: FRU Failure Analysis.
440	Embedded port hardware failed.	Go to MAP 0500: FRU Failure Analysis.
442	Embedded port anomaly detected.	No action required.
445	ASIC detected a system anomaly.	No action required.
453	New feature key installed.	No action required.
506	Fibre Channel port failure.	Go to MAP 0600: Port Failure and Link Incident Analysis.
507	Loopback diagnostics port failure.	Go to MAP 0600: Port Failure and Link Incident Analysis.
508	Fibre Channel port anomaly detected.	No action required.

Table 4: Event Codes versus Maintenance Action (Continued)

Event Code	Explanation	Action
510	SFP optical transceiver hot-insertion initiated.	No action required.
512	SFP optical transceiver nonfatal error.	Go to MAP 0600: Port Failure and Link Incident Analysis.
513	SFP optical transceiver hot-removal completed.	No action required.
514	SFP optical transceiver failure.	Go to MAP 0600: Port Failure and Link Incident Analysis.
523	FL_Port open request failed.	No action required.
524	No AL_PA acquired.	No action required.
525	FL_Port arbitration timeout.	No action required.
581	Implicit incident.	Go to MAP 0600: Port Failure and Link Incident Analysis.
582	Bit error threshold exceeded.	Go to MAP 0600: Port Failure and Link Incident Analysis.
583	Loss of signal or loss of synchronization.	Go to MAP 0600: Port Failure and Link Incident Analysis.
584	Not operational primitive sequence received.	Go to MAP 0600: Port Failure and Link Incident Analysis.
585	Primitive sequence timeout.	Go to MAP 0600: Port Failure and Link Incident Analysis.
586	Invalid primitive sequence received for current link state.	Go to MAP 0600: Port Failure and Link Incident Analysis.
810	High temperature warning (CTP thermal sensor).	Go to MAP 0500: FRU Failure Analysis.
811	Critically hot temperature warning (CTP thermal sensor).	Go to MAP 0500: FRU Failure Analysis.

MAP 0000: Start MAP

This MAP describes initial fault isolation for the Edge Switch 2/32. Fault isolation begins at the Internet-connected PC accessing the Embedded Web Server (EWS) interface, rack-mounted HAFM appliance running HAFM version 8.00.01, failed switch, or switch-attached host.

1

Prior to fault isolation, acquire the following from the customer:

- A system configuration drawing or planning worksheet that includes the HAFM appliance, switch, other HP products, and device connections.
- The location of the HAFM appliance and all switches.
- The internet protocol (IP) address, gateway address, and subnet mask for the switch reporting the problem.
- If performing fault isolation using the EWS interface, the administrator user name and password. Both are case sensitive and required when prompted at the Username and Password Required dialog box.
- If performing fault isolation using the HAFM appliance:
  - The Windows 2000 user name and password, required when prompted during any MAP or repair procedure that directs the HAFM appliance to be rebooted.
  - The user ID and maintenance password. Both are case sensitive and required when prompted at the HAFM Login dialog box.

Continue to the next step.

2

Are you at a PC with a web browser (such as Netscape Navigator or Microsoft Internet Explorer), an Internet connection to the switch reporting the problem, and communicating with the switch through the EWS interface?

YES	NO
↓	Go to step 19.

3

Is the web-browser PC powered on and communicating with the switch through the Internet connection and EWS interface?

NO	YES

↓ Go to step 5.

4

Boot the web-browser PC.

1. Power on the PC in accordance with the instructions delivered with the PC. The Windows desktop appears.
2. Launch the PC browser application by double-clicking the Netscape Navigator icon or Internet Explorer icon at the Windows desktop.
3. At the **Netsite** field (Netscape Navigator) or **Address** field (Internet Explorer), type `http://xxx.xxx.xxx.xxx`, where *xxx.xxx.xxx.xxx* is the IP address of the switch (obtained in step 1). The Username and Password Required dialog box appears (Figure 4).

Figure 4: Username and Password Required dialog box

4. Type the user name and password obtained in step 1, and click **OK**. The EWS interface opens with the **View** panel displayed (Figure 5).

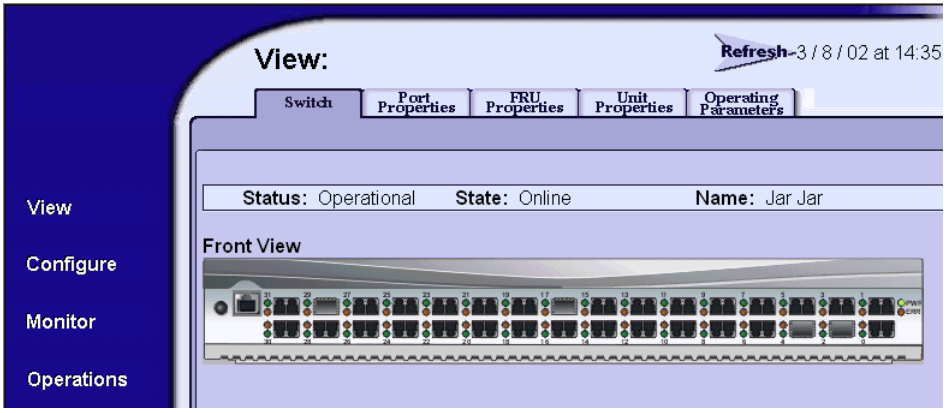


Figure 5: View Panel (EWS Interface)

Continue to the next step.

5

Does the EWS interface appear operational with the **View** panel displayed?

NO	YES
↓	Go to step 10.

6

A `Page cannot be found, Unable to locate the server, HTTP 404-file not found`, or other similar message appears. The message indicates the PC cannot communicate with the switch because:

- The switch-to-PC Internet link could not be established.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch control processor (CTP) card failed.

Continue to the next step.

7

Ensure the switch is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES	NO
↓	A power distribution problem is indicated. Go to "MAP 0100: Power Distribution Analysis" on page 51. Exit MAP.

8

At the front of the switch, inspect the amber **ERR** LED.

Is the LED illuminated?

NO	YES

↓ A FRU failure or link incident is indicated. Go to step 18 to obtain event codes that identify the failure. Exit MAP.

9

A switch-to-PC Internet link problem (Internet too busy or IP address typed incorrectly) is indicated.

1. Wait approximately five minutes, then attempt to login to the switch again.
2. At the **Netsite** field (Netscape Navigator) or **Address** field (Internet Explorer), type `http://`*`xxx.xxx.xxx.xxx`*, where *`xxx.xxx.xxx.xxx`* is the IP address of the switch (obtained in step 1). The Username and Password Required dialog box appears (Figure 4).
3. Type the user name and password obtained in step 1, and click **OK**. If the **View** panel does not display, wait another five minutes and perform this step again.

Does the EWS interface appear operational with the **View** panel displayed?

YES **NO**

↓ Perform switch fault isolation at the HAFM appliance. Go to step 20.

10

At the **View** panel, inspect the **Status** field.

Does the switch status indicate **Operational**?

NO **YES**

↓ The switch appears operational. Exit MAP.

11

Inspect Fibre Channel port operational states.

1. At the **View** panel, click the **Port Properties** tab. The **View** panel (**Port Properties** tab) displays with port **0** highlighted (Figure 6).

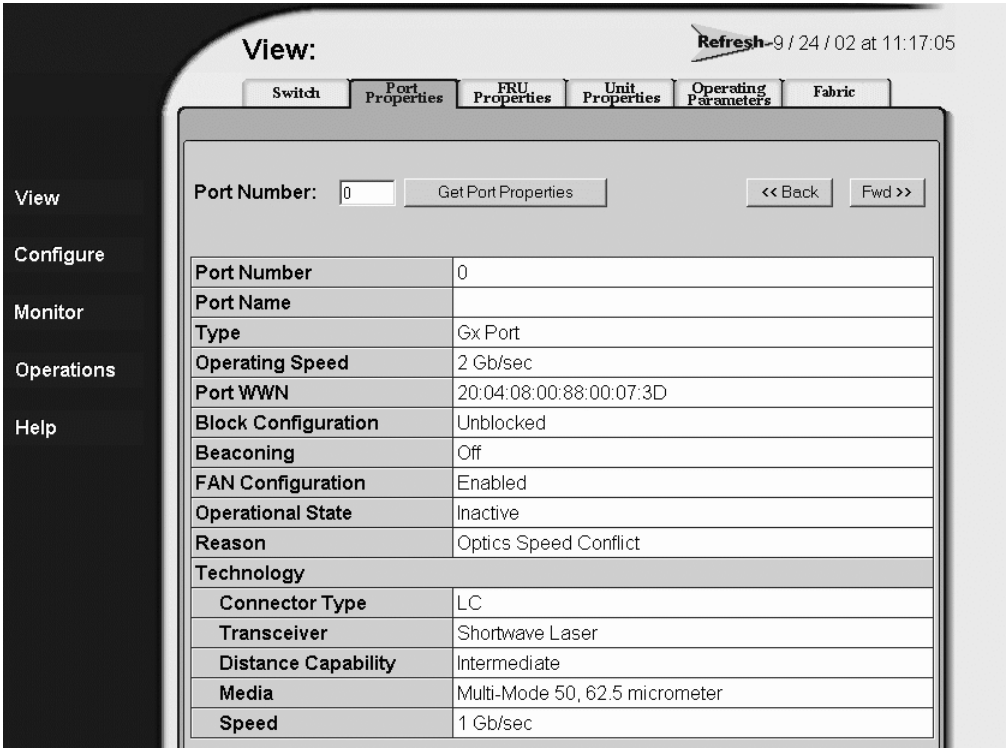


Figure 6: View Panel (Port Properties Tab)

2. Inspect the **Beaconing** and **Operational State** fields.

Does the **Beaconing** field display an `On` message?

YES	**NO**
↓	Go to step 13.

12

Port beaconing is enabled.

1. Consult the customer and next level of support to determine the reason port beaconing is enabled.
2. Disable port beaconing:
   a. At the **View** panel, click **Operations** at the left side of the panel. The **Operations** panel opens with the **Beaconing** page displayed.

b. Click the **Beaconing State** check box for the port. The check mark disappears and port beaconing is disabled.

c. Return to the **View** panel (**Port Properties** tab).

Continue to the next step.

13

At the **View** panel, does the **Operational State** field display a `Segmented` message?

NO **YES**

↓ Port segmentation is indicated. Go to step 18 to obtain event codes. If no event codes are found, go to "MAP 0700: Fabric, ISL, and Segmented Port Problem Determination" on page 107. Exit MAP.

14

At the **View** panel, does the **Operational State** field display a message indicating a port problem?

NO **YES**

↓ Go to step 18 to obtain event codes. If no event codes are found, go to "MAP 0600: Port Failure and Link Incident Analysis" on page 89. Exit MAP.

15

Repeat step 11 through step 14 for each remaining Fibre Channel port for which a problem is suspected (ports **0** through **31**).

Is a problem indicated for any of the ports?

NO **YES**

↓ Go to step 18 to obtain event codes. If no event codes are found, go to "MAP 0600: Port Failure and Link Incident Analysis" on page 89. Exit MAP.

16

Inspect power supply operational states.

1. At the **View** panel, click the **FRU Properties** tab. The **View** panel (**FRU Properties** tab) displays.
2. Inspect the **Status** fields for both power supplies.

Does the **Status** field display a `Failed` message for either power supply?

NO	YES
↓	A power supply failure is indicated. Go to step 18 to obtain event codes. If no event codes are found, go to "MAP 0100: Power Distribution Analysis" on page 51. Exit MAP.

17

Inspect the **Status** fields for switch FRUs.

Does the **State** field display a `Failed` message for any of the FRUs?

YES	NO
↓	The switch appears operational. Exit MAP.

A FRU failure is indicated. Continue to the next step to obtain event codes. If no event codes are found, go to "MAP 0500: FRU Failure Analysis" on page 83. Exit MAP.

18

Obtain event codes from the EWS Event Log.

Note: If multiple event codes are found, note all codes and associated severity levels. Record the date, time, and listed sequence, and determine if the codes are related to the reported problem. Begin fault isolation with the most recent event code with the highest severity level. Other codes may accompany this event code, or may indicate a normal indication after a problem is recovered.

1. At the **View** panel, click **Monitor** at the left side of the panel. The **Monitor** panel opens with the **Port List** page displayed.
2. At the **Monitor** panel, click the **Log** tab. The **Monitor** panel (**Log** tab) displays (Figure 7).

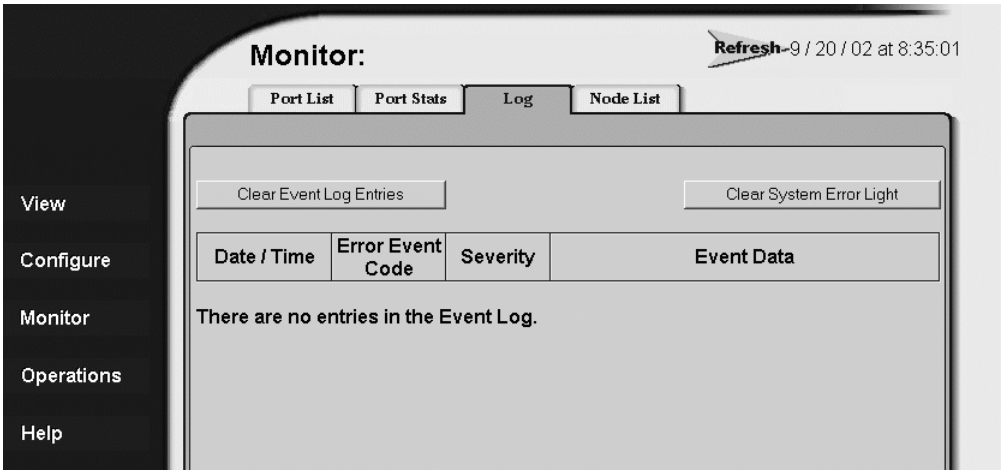


Figure 7: Monitor Panel (Log Tab)

3. Record the event code, date, time, and severity (**Informational**, **Minor**, **Major**, or **Severe**).
4. Record all event codes that may relate to the reported problem.

Were one or more event codes found?

NO	**YES**
↓	Go to Table 4 to interpret event codes. Exit MAP.

Return to step 1 and perform fault isolation again. If this is the second time at this step, contact the next level of support. Exit MAP.

19

Are you at the HAFM appliance?

YES	**NO**
↓	Go to step 39.

20

Did the HAFM appliance lock up or crash and:

- Display an application warning or error message, or
- Not display an application warning or error message, or
- Display a Dr. Watson for Windows 2000 dialog box?

NO	YES
↓	An HAFM appliance application problem is indicated. Event codes are not recorded. Go to "MAP 0300: HAFM Appliance Software Problem Determination" on page 61. Exit MAP.

21

Did the HAFM appliance crash and display a blue screen with the system dump file in hexadecimal format (blue screen of death)?

NO	YES
↓	An HAFM appliance application problem is indicated. Event codes are not recorded. Go to "MAP 0300: HAFM Appliance Software Problem Determination" on page 61. Exit MAP.

22

Is the HAFM active?

NO	YES
↓	Go to step 24.

23

Reboot the HAFM appliance.

1. At the Windows 2000 desktop, click **Start** at the left side of the task bar (bottom of the desktop), then click **Shut Down**. The Shut Down Windows dialog box displays
2. Click the **Shut Down** option from the list box and click **OK**. The HAFM appliance powers down.
3. Wait approximately 30 seconds and press the power (⏻) button on the liquid crystal display (LCD) panel to power on the HAFM appliance and perform power-on self-tests (POSTs). During POSTs:
   a. The green LCD panel illuminates.
   b. The green hard disk drive (**HDD**) LED blinks momentarily, and processor speed and random-access memory information display momentarily at the LCD panel.
   c. After a few seconds, the LCD panel displays the following message pertaining to boot sequence selection (Figure 8):

Figure 8: LCD panel during boot sequence

d. Ignore the message. After ten seconds, the HAFM appliance performs the boot sequence from the basic input/output system (BIOS). During the boot sequence, the HAFM appliance performs additional POSTs and displays the following operational information at the LCD panel:

   — Host name.

   — System date and time.

   — LAN 1 and LAN 2 IP addresses.

   — Fan rotational speed.

   — Central processing unit (CPU) temperature.

   — Hard disk capacity.

   — Virtual and physical memory capacity.

4. After successful POST completion, the LCD panel displays a `Welcome!!` message, then continuously cycles through and displays HAFM appliance operational information.

5. After rebooting the HAFM appliance at the LCD panel, log on to the HAFM appliance Windows 2000 desktop through a LAN connection to a browser-capable PC. Refer to the *HP StorageWorks Edge Switch 2/32 Installation Guide* for instructions on accessing the HAFM appliance desktop. The HAFM 8 Login dialog box displays (Figure 9).

Figure 9: HAFM 8 Login dialog box

6. Type a user ID and password (obtained in step 1, and both are case sensitive), and click **Login**. The *HAFM* application starts and the HAFM main window displays (Figure 10).

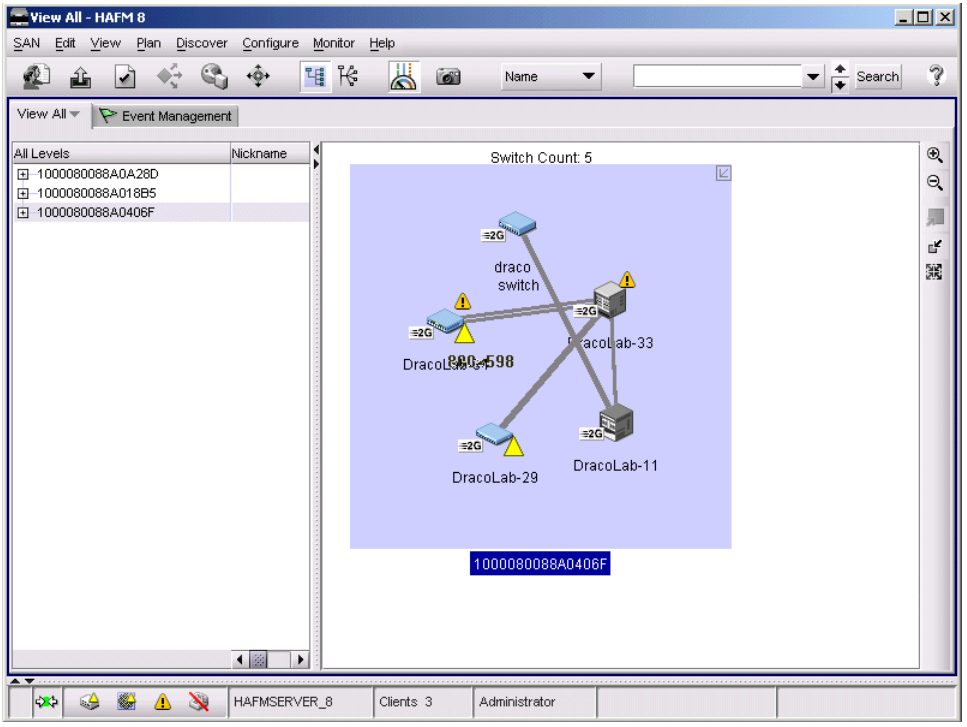


Figure 10: HAFM 8 main window

Did the main window display and does HAFM appear operational?

YES	NO
↓	An HAFM appliance problem is indicated. Event codes are not recorded. Go to "MAP 0800: HAFM Appliance or Web Browser PC Hardware Problem Determination" on page 122. Exit MAP.

24

Inspect the status symbol associated with the Edge Switch 2/32 at the main window's physical map or product list. The symbol shows the status of switch or the status of the link between the HAFM appliance and switch as follows:

- No status symbol indicates that the switch is operational.

- A yellow triangle indicates that the switch is operating in degraded mode.
- A red diamond indicates that the switch is not operational.
- A grey square with yellow exclamation mark indicates that the status of the switch is unknown.

Is a grey square with yellow exclamation mark associated with the icon representing the switch reporting the problem?

YES	NO
↓	Go to step 28.

The status symbol indicates the HAFM appliance cannot communicate with the switch because:

- The switch-to-HAFM appliance Ethernet link failed.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch CTP card failed.

Continue to the next step.

25

Ensure the switch is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES	NO
↓	A power distribution problem is indicated. Go to step 38 to obtain event codes. If no event codes are found, go to "MAP 0100: Power Distribution Analysis" on page 51. Exit MAP.

26

At the front of the switch, inspect the amber **ERR** LED.

Is the LED illuminated?

NO	YES
↓	A FRU failure or link incident is indicated. Go to step 38 to obtain event codes that identify the failure. Exit MAP.

27

A switch-to-HAFM appliance Ethernet link failure is indicated.

Go to step 38 to obtain event codes. If no event codes are found, go to "MAP 0400: Loss of HAFM Appliance or Web Browser PC Communication" on page 69. Exit MAP.

28

Is a red diamond (failure indicator) associated with the icon representing the switch reporting the problem?

YES	NO
↓	Go to step 30.

29

Right-click the icon representing the switch reporting the problem. A pop-up menu appears. Click the **Element Manager** option from the menu. The *Element Manager* application opens and the **Hardware View** displays.

At the **Hardware View**:

- Observe that the **Edge Switch Status** table is yellow and the switch status is **NOT OPERATIONAL**.
- Inspect FRUs for a blinking red and yellow diamond (failed FRU indicator) that overlays the FRU graphic.

Do blinking red and yellow diamonds overlay any FRU graphics?

NO	YES
↓	Failure of one or more FRUs is indicated. Go to step 38 to obtain event codes. If no event codes are found, go to "MAP 0500: FRU Failure Analysis" on page 83. Exit MAP.

30

Is a yellow triangle (attention indicator) associated with the icon representing the switch reporting the problem?

YES	NO
↓	Go to step 33.

31

Right-click the icon representing the switch reporting the problem. A pop-up menu appears. Click the **Element Manager** option from the menu. The *Element Manager* application opens and the **Hardware View** displays. At the **Hardware View**:

- Observe that the **Edge Switch Status** table is yellow and the switch status is **Minor Failure** or **Redundant Failure**.
- Inspect FRUs for a blinking red and yellow diamond (failed FRU indicator) that overlays the FRU graphic.

Does a blinking red and yellow diamond overlay a power supply graphic?

NO	YES
↓	A power supply failure is indicated. Go to step 38 to obtain event codes. If no event codes are found, go to "MAP 0100: Power Distribution Analysis" on page 51. Exit MAP.

32

Does a blinking red and yellow diamond overlay a port graphic?

NO	YES
↓	A port failure is indicated. Go to step 38 to obtain event codes. If no event codes are found, go to "MAP 0600: Port Failure and Link Incident Analysis" on page 89. Exit MAP.

33

No colored status symbol is associated the icon representing the switch reporting the problem. Although the switch is operational, a minor problem may exist.

Right-click the icon representing the switch reporting the problem. A pop-up menu appears. Click the **Element Manager** option from the menu. The *Element Manager* application opens and the **Hardware View** displays. At the **Hardware View**:

- Inspect the switch for a yellow triangle that overlays the FRU graphic and indicates FRU beaconing is enabled.
- Inspect ports for a yellow triangle (attention indicator) that overlays the port graphic.

Does a yellow triangle overlay the switch or FRU graphic?

YES	NO

↓ Go to step 35.

34

Beaconing is enabled for the FRU.

1. Consult the customer and next level of support to determine the reason FRU beaconing is enabled.
2. Disable FRU beaconing.
   a. At the **Hardware View**, right-click the FRU graphic. A pop-up menu appears.
   b. Click the **Enable Beaconing** option. The check mark disappears from the box adjacent to the option, and FRU beaconing is disabled.

Was FRU beaconing enabled because FRU failure or degradation was suspected?

YES **NO**

↓ The switch appears operational. Exit MAP.

Go to step 20 and perform fault isolation again (through the HAFM appliance).

35

Does a yellow triangle (attention indicator) overlay a port graphic?

YES **NO**

↓ Go to step 37.

36

Inspect the port state and LED status for all ports with an attention indicator.

1. Double-click a port to open the Port Properties dialog box (Figure 11).

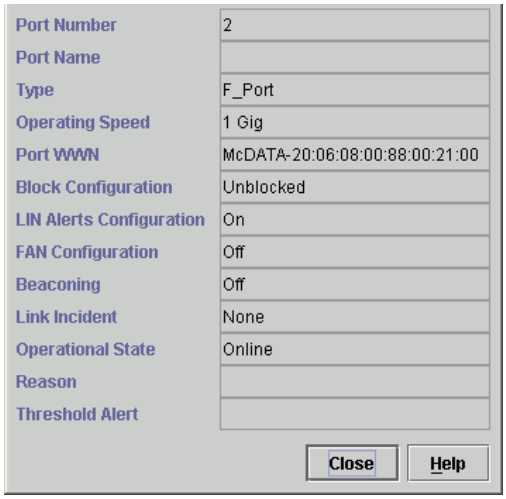


Figure 11: Port Properties dialog box

2. Inspect the **Operational State** field.

Does the **Operational State** field display a `Segmented E_Port` message?

NO	YES
↓	Expansion port (E_Port) segmentation is indicated. Go to step 38 to obtain event codes. If no event codes are found, go to "MAP 0700: Fabric, ISL, and Segmented Port Problem Determination" on page 107. Exit MAP.

A message displays indicating a link incident problem. Go to step 38 to obtain event codes. If no event codes are found, go to "MAP 0600: Port Failure and Link Incident Analysis" on page 89. Exit MAP.

37

A link incident (LIN) may have occurred, but the LIN alerts option is not enabled for the port and the attention indicator does not appear.

At the **Hardware View**, click **Logs > Link Incident Log**. The Link Incident Log displays (Figure 12).

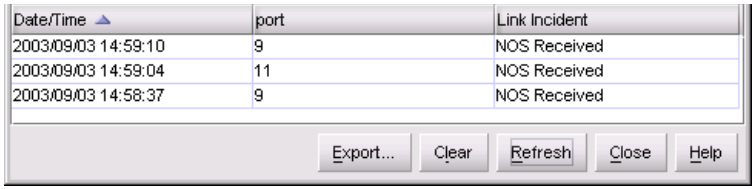


Figure 12: Link Incident Log

If a link incident occurred, the affected port number is listed with one of the following messages.

- `Link interface incident - implicit incident`
- `Link interface incident - bit-error threshold exceeded`
- `Link failure - loss of signal or loss of synchronization`
- `Link failure - not-operational primitive sequence (NOS) received`
- `Link failure - primitive sequence timeout`
- `Link failure - invalid primitive sequence received for the current link state`

Did one of the listed messages appear in the Link Incident Log?

YES	NO
↓	The switch appears operational. Exit MAP.

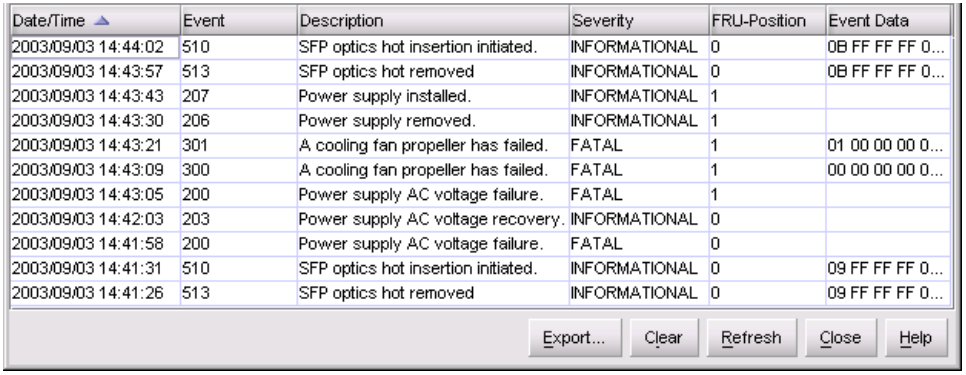
A link incident problem is indicated. Continue to the next step to obtain event codes. If no event codes are found, go to "MAP 0700: Fabric, ISL, and Segmented Port Problem Determination" on page 107. Exit MAP.

38

Obtain event codes from the Edge Switch Event Log.

Note: If multiple event codes are found, note all codes and associated severity levels. Record the date, time, and listed sequence, and determine if the codes are related to the reported problem. Begin fault isolation with the most recent event code with the highest severity level. Other codes may accompany this event code, or may indicate a normal indication after a problem is recovered.

1. At the **Hardware View**, click **Logs > Event Log**. The Event Log displays (Figure 13).



Date/Time	Event	Description	Severity	FRU-Position	Event Data
2003/09/03 14:44:02	510	SFP optics hot insertion initiated.	INFORMATIONAL	0	0B FF FF FF 0...
2003/09/03 14:43:57	513	SFP optics hot removed	INFORMATIONAL	0	0B FF FF FF 0...
2003/09/03 14:43:43	207	Power supply installed.	INFORMATIONAL	1	
2003/09/03 14:43:30	206	Power supply removed.	INFORMATIONAL	1	
2003/09/03 14:43:21	301	A cooling fan propeller has failed.	FATAL	1	01 00 00 00 0...
2003/09/03 14:43:09	300	A cooling fan propeller has failed.	FATAL	1	00 00 00 00 0...
2003/09/03 14:43:05	200	Power supply AC voltage failure.	FATAL	1	
2003/09/03 14:42:03	203	Power supply AC voltage recovery.	INFORMATIONAL	0	
2003/09/03 14:41:58	200	Power supply AC voltage failure.	FATAL	0	
2003/09/03 14:41:31	510	SFP optics hot insertion initiated.	INFORMATIONAL	0	09 FF FF FF 0...
2003/09/03 14:41:26	513	SFP optics hot removed	INFORMATIONAL	0	09 FF FF FF 0...

Export... Clear Refresh Close Help

Figure 13: Event Log

2. Record the event code, date, time, and severity (**Informational**, **Minor**, **Major**, **Severe**, or **Fatal**).
3. Record all event codes that may relate to the reported problem.

Were one or more event codes found?

NO **YES**

↓ Go to Table 4 on page 24 to interpret event codes. Exit MAP.

Return to step 1 and perform fault isolation again. If this is the second time at this step, contact the next level of support. Exit MAP.

39

Are you at the switch reporting the problem?

YES **NO**

↓ Go to step 51.

40

Is the green **PWR** LED at the switch front bezel illuminated?

NO	YES
↓	Go to step 45.

41

Is the switch connected to facility AC power and powered on?

NO	YES
↓	Go to step 44.

42

Connect the switch to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES	NO
↓	A power distribution problem is indicated. Go to step 38 to obtain event codes. If no event codes are found, go to "MAP 0100: Power Distribution Analysis" on page 51. Exit MAP.

43

Is the green **PWR** LED at the switch front bezel illuminated?

NO	YES
↓	Go to step 45.

A faulty **PWR** LED is indicated, but switch and Fibre Channel port operation is not disrupted. The LED is connected to CTP card circuitry, and if this problem is a concern to the customer, the switch must be replaced. Exit MAP.

44

Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).

- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES	NO
↓	A power distribution problem is indicated. Go to step 38 to obtain event codes. If no event codes are found, go to "MAP 0100: Power Distribution Analysis" on page 51. Exit MAP.

A faulty **PWR** LED is indicated, but switch and Fibre Channel port operation is not disrupted. The LED is connected to CTP card circuitry, and if this problem is a concern to the customer, the switch must be replaced. Exit MAP.

45

Is the amber **ERR** LED at the switch front bezel blinking?

YES	NO
↓	Go to step 47.

46

Unit beaconing is enabled for the switch.

1. Consult the customer and next level of support to determine the reason unit beaconing is enabled.
2. Disable unit beaconing.
   a. At the **Hardware View**, right-click the front bezel graphic (away from a FRU). A pop-up menu appears.
   b. Click the **Enable Unit Beaconing** option. The check mark disappears from the box adjacent to the option, and unit beaconing is disabled.

Was unit beaconing enabled because switch failure or degradation was suspected?

YES	NO
↓	The switch appears operational. Exit MAP.

Go to step 39 and perform fault isolation again (at the switch).

47

Is the amber **ERR** LED at the switch front bezel illuminated?

YES	NO
↓	The switch appears operational. Verify switch operation at the HAFM appliance. Go to step 20.

48

Check FRUs for failure symptoms.

Are any amber LEDs associated with Fibre Channel ports illuminated?

NO	YES
↓	A Fibre Channel port failure is indicated. Go to step 38 to obtain event codes. If no event codes are found, go to "MAP 0600: Port Failure and Link Incident Analysis" on page 89. Exit MAP.

49

Is the amber **ERR** LED at the front of the switch illuminated?

NO	YES
↓	A FRU failure or link incident is indicated. Go to step 38 to obtain event codes that identify the failure. Exit MAP.

50

Is the amber LED on a power supply illuminated?

NO	YES
↓	A power supply failure is indicated. Go to step 38 to obtain event codes. If no event codes are found, go to "MAP 0100: Power Distribution Analysis" on page 51. Exit MAP.

The switch appears operational. Exit MAP.

51

You are at the console of an open systems interconnection (OSI) server attached to the switch reporting the problem. If an incident occurs on the Fibre Channel link between the switch and server, a link incident record is generated and sent to the server using the reporting procedure defined in T11/99-017v0.

Was a link incident record generated and sent to the switch-attached OSI server?

YES	NO
↓	Perform switch fault isolation at the HAFM appliance. Go to step 20.

52

The link incident record provides the attached switch port number(s) and one or more of the following event codes and messages. Record all event codes that may relate to the reported problem.

- 581 - `Link interface incident - implicit incident`
- 582 - `Link interface incident - bit-error threshold exceeded`
- 583 - `Link failure - loss of signal or loss of synchronization`
- 584 - `Link failure - not-operational primitive sequence (NOS) received`
- 585 - `Link failure - primitive sequence timeout`
- 586 - `Link failure - invalid primitive sequence received for the current link state`

Were one or more event codes found?

YES	NO
↓	Perform switch fault isolation at the HAFM appliance. Go to step 20.

Go to Table 4 on page 24 to interpret event codes. Exit MAP.

MAP 0100: Power Distribution Analysis

This MAP describes fault isolation for the switch power distribution system, including defective AC power cords or redundant power supplies.

1

Was an event code **200** or **201**, **202**, **208** observed at the EWS Event Log or at the Edge Switch Event Log (HAFM appliance)?

YES **NO**

↓ Go to step 9.

2

Table 5 lists event codes, brief explanations of the codes, and the associated steps that describe fault isolation procedures.

Table 5: MAP 100 Event Codes

Event Code	Explanation	Action
200	Power supply AC voltage failure.	Go to step 3.
201	Power supply DC voltage failure.	Go to step 8.
202	Power supply thermal failure.	Go to step 8.
208	Power supply false shutdown.	Go to step 3.

3

Have the customer inspect and verify that facility power is within specifications. These specifications are:

- One single-phase connection for each power supply.
- Input power between 100 and 240 VAC, and at least 5 amps.
- Input frequency between 47 and 63 Hz.

Is facility power within specifications?

YES **NO**

↓ Ask the customer to correct the facility power problem. When facility power is corrected, continue to the next step.

4

A redundant power supply is disconnected from facility power, not properly installed, or has failed. Verify the power supply is connected to facility power.

1. Ensure the AC power cord associated with the power supply (**PS0** or **PS1**) is connected to the rear of the switch and a facility power receptacle. If not, connect the cord as directed by the customer.
2. Ensure the associated facility circuit breaker is on. If not, ask the customer set the circuit breaker on.
3. Ensure the AC power cord is not damaged. If damaged, replace the cord.

Was a corrective action performed?

YES	NO
↓	Go to step 6.

5

Verify redundant power supply operation.

1. Inspect the power supply and ensure the green LED illuminates.
2. At the HAFM appliance **Hardware View**, observe the graphic representing the power supply and ensure a failure symbol (blinking red and yellow diamond) does not appear.

Is a failure indicated?

YES	NO
↓	The switch appears operational. Exit MAP.

6

Ensure the indicated power supply is correctly installed and seated in the switch. If required, partially remove and reseat the power supply.

Was a corrective action performed?

YES	NO
↓	Go to step 8.

7

Verify redundant power supply operation.

1. Inspect the power supply and ensure the green LED illuminates.

2. At the HAFM appliance **Hardware View**, observe the graphic representing the power supply and ensure a failure symbol (blinking red and yellow diamond) does not appear.

Is a failure indicated?

YES **NO**

↓ The switch appears operational. Exit MAP.

8

Visual inspection or an event code **200** or **201** indicates one or both power supplies must be removed and replaced. Refer to "RRP: Power Supply" on page 186.

- This procedure is concurrent and can be performed while switch power is on.
- Perform the data collection procedure as part of FRU removal and replacement.
- If multiple power supply failures occurred, connect the switch to facility AC power after both power supplies are replaced.

Caution: Do not remove a power supply unless a replacement FRU is immediately available. To avoid product overheating, a removed power supply must be replaced within five minutes.

Did power supply replacement solve the problem?

NO **YES**

↓ The switch appears operational. Exit MAP.

Contact the next level of support. Exit MAP.

9

Is fault isolation being performed at the switch?

YES **NO**

↓ Fault isolation is being performed at the EWS interface or HAFM appliance. Go to step 18.

10

Verify the switch is connected to facility power and is powered on.

1. Ensure the AC power cord associated with the power supply (**PS0** or **PS1**) is connected to the rear of the switch and a facility power receptacle. If not, connect the cord as directed by the customer.
2. Ensure the associated facility circuit breaker is on. If not, ask the customer set the circuit breaker on.
3. Ensure the AC power cord is not damaged. If damaged, replace the cord.

Continue to the next step.

11

Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** or **ERR** indicator.
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES	**NO**
↓	Go to step 13.

12

Does inspection of a power supply indicate a failure (green LED is extinguished)?

NO	**YES**
↓	A redundant power supply failed. Go to step 8.

The switch appears operational. Exit MAP.

13

The switch AC power distribution system failed. Possible causes include failure of:

- Both power supplies.
- The CTP card.

Does inspection of both power supplies indicate a dual failure (green LED extinguished on each power supply)?

YES	NO
↓	One or both power supplies appear operational, but a power distribution failure through the CTP card is indicated. Go to step 17.

14

Ensure both power supplies are correctly installed and seated in the switch. If required, partially remove and reseat the power supplies. Refer to "RRP: Power Supply" on page 186.

Was a corrective action performed?

YES	NO
↓	Go to step 16.

15

Verify operation of both power supplies.

1. Inspect the power supplies and ensure the green LED is illuminated.
2. At the HAFM appliance **Hardware View**, observe the graphics representing the power supplies and ensure a failure symbol (blinking red and yellow diamond) does not appear.

Is a dual power supply failure still indicated?

YES	NO
↓	The switch appears operational. Exit MAP.

16

Both power supplies failed and must be removed and replaced. Refer to "RRP: Power Supply" on page 186.

- Perform the data collection procedure as part of FRU removal and replacement.
- Connect the switch to facility AC power after both power supplies are replaced.

Did dual power supply replacement solve the problem?

NO	YES
↓	The switch appears operational. Exit MAP.

A dual power supply failure is not confirmed. Replace both original power supplies to avoid the cost of expending replacement FRUs. Continue to the next step.

17

One or both power supplies appear operational, but the CTP card is not receiving DC power. The in-card circuit breaker may have tripped due to a power surge, or the CTP card failed.

Disconnect both power cords, then reconnect the power cords (power cycle the switch) to reset the CTP card.

Did power cycling the switch solve the problem?

NO	YES
↓	The switch appears operational. Exit MAP.

Analysis for a CTP card failure is not described in this MAP. Go to "MAP 0000: Start MAP" on page 29. Exit MAP.

18

Is fault isolation being performed at the EWS interface?

YES	NO
↓	Fault isolation is being performed at the HAFM appliance. Go to step 23.

19

Does the EWS interface appear operational?

NO	YES
↓	Go to step 22.

20

A `Page cannot be found, Unable to locate the server, HTTP 404 - file not found`, or other similar message appears. The message indicates the PC cannot communicate with the switch because:

- The switch-to-PC Internet link could not be established.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch CTP card failed.

Continue to the next step.

21

Ensure the switch reporting the problem is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES **NO**

↓ Go to step 13.

Analysis for an Ethernet link or a CTP failure is not described in this MAP. Go to "MAP 0000: Start MAP" on page 29. If this is the second time at this step, contact the next level of support. Exit MAP.

22

Inspect power supply operational states at the EWS interface.

1. At the **View** panel, click the **FRU Properties** tab. The **View** panel (**FRU Properties** tab) displays.
2. Inspect the **Status** fields for both power supplies.

Does the **Status** field display a `Failed` message for either power supply?

NO **YES**

↓ A redundant power supply failed. Go to step 8.

The switch appears operational. Exit MAP.

23

At the HAFM appliance **Hardware View**, does a yellow triangle appear at the alert panel and a blinking red and yellow diamond (failed FRU indicator) appear to overlay a power supply graphic?

NO **YES**

↓ A redundant power supply failed. Go to step 8.

24

At the **Hardware View**, does a grey square appear at the alert panel, a **No Link** status appear at the **Edge Switch Status** table, and graphical FRUs appear uninstalled?

YES	NO
↓	A green circle appears at the alert panel and the switch appears operational. Exit MAP.

The grey square indicates the HAFM appliance cannot communicate with the switch because:

- The switch-to-HAFM appliance Ethernet link failed.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch CTP card failed.

Continue to the next step.

25

Ensure the switch is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES	NO
↓	Go to step 13.

Analysis for an Ethernet link or a CTP failure is not described in this MAP. Go to "MAP 0000: Start MAP" on page 29. If this is the second time at this step, contact the next level of support. Exit MAP.

MAP 0200: POST Failure Analysis

When the switch is powered on, it performs a series of power-on self-tests (POSTs). When POSTs complete, the switch performs an initial program load (IPL) that loads firmware and brings the unit online. This MAP describes fault isolation for problems that may occur during the POST/IPL process.

If an error is detected, the POST/IPL process continues in an attempt to initialize the switch and bring it online. But an event code **400** displays when the switch completes the POST/IPL process.

1

Was an event code **400** or **411** observed at the switch **Event Log** (HAFM appliance) or at the **Embedded Web Server Event Log**?

YES **NO**

↓ Analysis for the failure is not described in this MAP. Go to "MAP 0000: Start MAP" on page 29. Exit MAP.

2

The following table lists event codes, brief explanations of the codes, and the associated steps that describe fault isolation procedures.

Table 6: MAP 200: Event Codes

Event Code	Explanation	Action
400	Power-up diagnostic failure.	Go to step 3.
411	Firmware fault occurred.	Go to step 4.

3

POST/IPL diagnostics detected a CTP failure as indicated by an event code **400** with supplementary bytes of event data.

- Byte 0 is a FRU code (02) that indicates a failed CTP.
- Byte 1 is the slot number (00) for the CTP.

Because the CTP card is not a FRU, CTP failure requires replacing the switch.

4

POST/IPL diagnostics detected a firmware failure (as indicated by event code **411**) and performed an online dump. All Fibre Channel ports reset after the failure and attached devices momentarily log out, log in, and resume operation.

Perform the data collection procedure and return the backup disk to HP support personnel. Exit MAP.

MAP 0300: HAFM Appliance Software Problem Determination

This map describes isolation of HAFM appliance application problems, including those associated with the Windows 2000 Professional operating system, *HAFM* application, or Edge Switch 2/32 *Element Manager* application.

1

Did the HAFM appliance lock up or crash without displaying a warning or error message?

YES	NO
↓	Go to step 4.

2

An application or operating system problem is indicated. Close HAFM (at the browser-capable PC connected through an Ethernet LAN segment to the HAFM appliance).

1. At the HAFM appliance Windows 2000 desktop, click the **Send Ctrl-Alt-Del** button at the top of the window. The Windows Security dialog box displays (Figure 14).

Note: Do not simultaneously press the **Ctrl**, **Alt**, and **Delete** keys. This action controls the browser-capable PC, not the HAFM appliance.

Figure 14: Windows Security dialog box

2. Click **Task Manager**. The Windows Task Manager dialog box displays with the **Applications** page open by default (Figure 15).

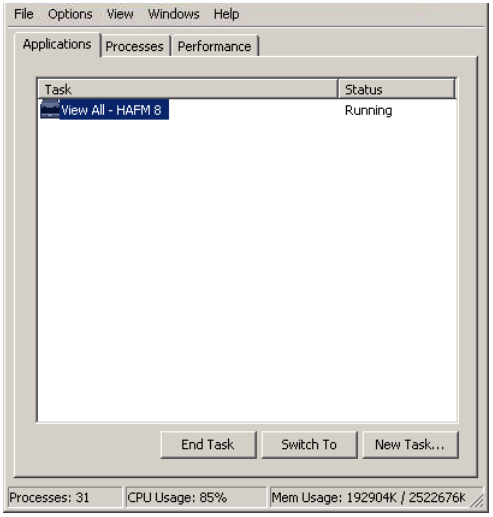


Figure 15: Windows Task Manager dialog box (Applications page)

3. Select (highlight) the **HAFM** entry and click **End Task**. HAFM closes.

Continue to the next step.

3

Attempt to clear the problem by rebooting the HAFM appliance.

1. At the Windows 2000 desktop, click **Start** at the left side of the task bar (bottom of the desktop), then click **Shut Down**. The Shut Down Windows dialog box displays.
2. Click the **Shut Down** option from the list box and click **OK**. The HAFM appliance powers down.
3. Wait approximately 30 seconds and press the power (⏻) button on the LCD panel to power on the HAFM appliance and perform POSTs. During POSTs:
   a. The green LCD panel illuminates.
   b. The green **HDD** LED blinks momentarily, and processor speed and random-access memory information display momentarily at the LCD panel.

c. After a few seconds, the LCD panel displays the following message pertaining to boot sequence selection (Figure 16):

Figure 16: LCD panel during boot sequence

d. Ignore the message. After ten seconds, the HAFM appliance performs the boot sequence from the BIOS. During the boot sequence, the HAFM appliance performs additional POSTs and displays the following operational information at the LCD panel:

   — Host name.
   — System date and time.
   — LAN 1 and LAN 2 IP addresses.
   — Fan rotational speed.
   — CPU temperature.
   — Hard disk capacity.
   — Virtual and physical memory capacity.

4. After successful POST completion, the LCD panel displays a `Welcome!!` message, then continuously cycles through and displays HAFM appliance operational information.
5. After rebooting the HAFM appliance at the LCD panel, log on to the HAFM appliance Windows 2000 desktop through a LAN connection to a browser-capable PC. Refer to the *HP StorageWorks Edge Switch 2/32 Installation Guide* for instructions on accessing the HAFM appliance desktop. HAFM starts and the HAFM Login dialog box displays.
6. Type a user ID and password (obtained in "MAP 0000: Start MAP" on page 29, and both are case sensitive), and click **Login**. HAFM opens and the HAFM main window displays.

Did the main window display and does HAFM appear operational?

NO	**YES**
↓	The problem is transient and the HAFM appliance appears operational. Exit MAP.

Contact the next level of support. Exit MAP.

4

Did HAFM display a dialog box with the message `Connection to management server lost - click OK to exit application or HAFM error n` (where *n* is an error message number **1** through **8** inclusive)?

NO	YES
↓	An *HAFM* application error occurred. Click **OK** to close the window and close the application. Go to step 3.

5

Did HAFM display a window with the message `The software version on this management server is not compatible with the version on the remote management server`?

YES	NO
↓	Go to step 8.

6

HAFM running on the HAFM appliance and client workstation are not at compatible release levels. Recommend to the customer that the downlevel version be upgraded.

Does the customer want HAFM upgraded?

YES	NO
↓	Power off the client workstation. Exit MAP.

7

Upgrade the downlevel HAFM. Refer to "Install or Upgrade Software" on page 175.

Did the software upgrade solve the problem?

NO	YES
↓	The HAFM appliance appears operational. Exit MAP.

Contact the next level of support. Exit MAP.

8

Did the *Element Manager* application display a window with the message `Element Manager error 5001` or `Element Manager error 5002`?

NO	YES
↓	An *Element Manager* application error occurred. Click **OK** to close the window and close the SAN management and *Element Manager* applications. Go to step 3.

9

Did the *Element Manager* application display a window with the message `Send firmware failed`?

YES	NO
↓	Go to step 11.

10

An attempt to download a firmware version from the HAFM appliance hard drive to the switch failed. Retry the operation. Refer to "Block and Unblock Ports" on page 161.

Did the firmware version download to the switch?

NO	YES
↓	The HAFM appliance appears operational. Exit MAP.

A CTP card failure is suspected. Go to "MAP 0000: Start MAP" on page 29 to isolate the problem. Exit MAP.

11

Did the *Element Manager* application display a window with the message `The data collection process failed`?

YES	NO
↓	Go to step 13.

12

The data collection process failed. Retry the process using a new CD. Refer to "Collecting Maintenance Data" on page 151.

Did the data collection process complete?

NO **YES**

↓ Exit MAP.

Contact the next level of support. Exit MAP.

13

Did the HAFM appliance lock up or crash and display a Dr. Watson for Windows 2000 dialog box (Figure 17)?

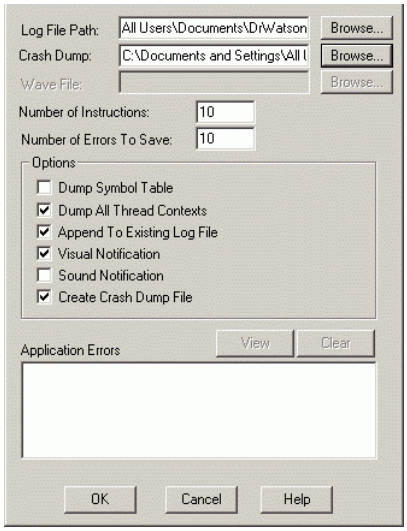


Figure 17: Dr. Watson for Windows 2000 dialog box

YES **NO**

↓ Go to step 14.

An *HAFM* application error occurred and transmitted a handling exception event to the operating system.

1. Click **Cancel** to close the Dr. Watson for Windows 2000 dialog box and HAFM.
2. Using the **My Computer** function at the Windows 2000 desktop, copy the crash dump file (*user.dmp*) from the local disk (*C:*) to the CD-RW drive (*D:*).
3. At the HAFM appliance, press the left edge (**PUSH** label) of the LCD panel to disengage the panel and expose the CD-RW drive.
4. Remove the CD and return it to HP customer support personnel for analysis.

Go to step 3.

14

Did the HAFM appliance crash and display a blue screen with the system dump file in hexadecimal format (blue screen of death)?

YES	NO
↓	The HAFM appliance appears operational. Exit MAP.

15

Attempt to clear the problem by power cycling the HAFM appliance.

1. At the HAFM appliance, press the power (⏻) button on the LCD panel to power off the HAFM appliance.
2. Wait approximately 30 seconds and press the power (⏻) button to power on the HAFM appliance and perform POSTs. During POSTs:
   a. The green LCD panel illuminates.
   b. The green **HDD** LED blinks momentarily, and processor speed and random-access memory information display momentarily at the LCD panel.
   c. After a few seconds, the LCD panel displays the following message pertaining to boot sequence selection (Figure 18):

Figure 18: LCD panel during boot sequence

   d. Ignore the message. After ten seconds, the HAFM appliance performs the boot sequence from BIOS. During the boot sequence, the HAFM appliance performs additional POSTs and displays the following operational information at the LCD panel:
      — Host name.
      — System date and time.
      — LAN 1 and LAN 2 IP addresses.
      — Fan rotational speed.
      — CPU temperature.
      — Hard disk capacity.

— Virtual and physical memory capacity.

3. After successful POST completion, the LCD panel displays a `Welcome!!` message, then continuously cycles through and displays HAFM appliance operational information.
4. After rebooting the HAFM appliance at the LCD panel, log on to the HAFM appliance's Windows 2000 desktop through a LAN connection to a browser-capable PC. Refer to the *HP StorageWorks Edge Switch 2/32 Installation Guide* for instructions on accessing the HAFM appliance desktop. HAFM starts and the HAFM Login dialog box displays
5. Type a user ID and password (obtained in "MAP 0000: Start MAP on page 29, and both are case sensitive), and click **Login**. HAFM opens and the HAFM main window displays.

Did the main window display and does HAFM appear operational?

NO	**YES**
↓	The problem is transient and the HAFM appliance appears operational. Exit MAP.

Contact the next level of support. Exit MAP.

MAP 0400: Loss of HAFM Appliance or Web Browser PC Communication

This MAP describes fault isolation of the Ethernet communication link between a switch and the HAFM appliance, or between a switch and a web browser PC running the EWS interface. Failure indicators include:

- Event codes recorded at the EWS Event Log or Edge Switch Event Log.
- At the web browser PC, A `Page cannot be found, Unable to locate the server, HTTP 404 - file not found`, or other similar message.
- At the HAFM main window, a grey square with an exclamation mark associated with the icon representing the switch reporting the problem.
- At the **Hardware View**, a grey square at the alert panel, a `No Link` status and reason at the **Edge Switch Status** table, and no FRUs visible for the switch.

When the logical connection between the switch and HAFM appliance is initiated, it may take up to five minutes for the link to activate at the HAFM main window. This delay is normal.

Caution: Prior to servicing a product or HAFM appliance, determine the Ethernet LAN configuration. Installation of products and servers on a public customer intranet can complicate problem determination and fault isolation.

1

Is fault isolation being performed at the EWS interface?

YES	NO
↓	Fault isolation is being performed at the HAFM appliance. Go to step 7.

2

Does the EWS interface appear operational?

NO	YES
↓	The switch-to-EWS PC connection is restored and appears operational. Exit MAP.

3

A `Page cannot be found, Unable to locate the server, HTTP 404 - file not found`, or other similar message appears. The message indicates the PC cannot communicate with the switch because:

- The switch-to-PC Internet (Ethernet) link could not be established.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch CTP card failed.

Continue to the next step.

4

Ensure the switch is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES	**NO**
↓	A power distribution problem is indicated. Go to "MAP 0100: Power Distribution Analysis" on page 51. Exit MAP.

5

At the front of the switch, inspect the amber **ERR** LED.

Is the LED illuminated?

NO	**YES**
↓	A FRU failure or link incident is indicated. Go to "MAP 0000: Start MAP" on page 29. Exit MAP.

6

Either a switch-to-PC Internet link problem (Internet too busy or IP address typed incorrectly) or a switch Ethernet port failure is indicated.

1. Wait approximately five minutes, then attempt to login to the switch again.

2. At the **Netsite** field (Netscape Navigator) or **Address** field (Internet Explorer), type `http://xxx.xxx.xxx.xxx`, where *xxx.xxx.xxx.xxx* is the IP address of the switch (obtained in "MAP 0000: Start MAP" on page 29). The Username and Password Required dialog box appears.
3. Type the user name and password obtained in "MAP 0000: Start MAP" on page 29 and click **OK**. If the **View** panel does not display, wait five minutes and perform this step again.

Does the EWS interface appear operational with the **View** panel displayed?

NO	**YES**
↓	The switch-to-EWS PC connection is restored and appears operational. Exit MAP.

Failure of the switch Ethernet port is indicated. Replace the switch. Exit MAP.

7

At the HAFM main window's physical map or product list is a grey square with yellow exclamation mark associated with the icon representing the switch reporting the problem?

YES	**NO**
↓	The switch-to-HAFM appliance connection is restored and appears operational. Exit MAP.

The status symbol indicates the HAFM appliance cannot communicate with the switch because:

- The switch-to-HAFM appliance Ethernet link failed.
- AC power distribution in the switch failed, or AC power was disconnected.
- The switch CTP card failed.

Continue to the next step.

8

Ensure the switch reporting the problem is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES **NO**

↓ A power distribution problem is indicated. Go to "MAP 0100: Power Distribution Analysis" on page 51. Exit MAP.

9

At the front of the switch, inspect the amber **ERR** LED.

Is the LED illuminated?

NO **YES**

↓ A FRU failure or link incident is indicated. Go to "MAP 0000: Start MAP" on page 29. Exit MAP.

10

The switch-to-HAFM appliance Ethernet link failed. At the physical map, right-click the icon with the grey square and exclamation mark representing the switch reporting the problem. A pop-up menu appears. Click the **Element Manager** option from the menu. The *Element Manager* application opens and the **Hardware View** displays. At the **Hardware View**:

- A grey square appears at the alert panel.
- No FRUs are visible for the switch.
- The **Edge Switch Status** table is yellow, the **Status** field displays **No Link**, and the **Reason** field displays an error message.

Table 7 lists the error messages and associated steps that describe fault isolation procedures.

Table 7: MAP 400 Error Messages

Error Message	Action
Never connected.	Go to step 11.
Link timeout.	Go to step 11.
Protocol mismatch.	Go to step 18.
Duplicate session.	Go to step 21.
Unknown network address.	Go to step 24.
Incorrect product type.	Go to step 26.

11

Transmit or receive errors for a switch's Ethernet adapter exceeded a threshold, the switch-to-HAFM appliance link was not connected, or the switch-to-HAFM appliance link timed out. A problem with the Ethernet cable, Ethernet hub or hubs, or other LAN-attached device is indicated.

Verify the switch is connected to the HAFM appliance through one or more Ethernet hubs.

1. Ensure an RJ-45 Ethernet cable connects the switch to an Ethernet hub. If not, connect the cables as directed by the customer.
2. Ensure an RJ-45 Ethernet cable connects the HAFM appliance to an Ethernet hub. If not, connect the cable as directed by the customer.
3. Ensure the Ethernet cables are not damaged. If damaged, replace the cables.

Was a corrective action performed?

NO	**YES**
↓	Go to step 1.

12

Does the LAN configuration use multiple (up to four) Ethernet hubs that are daisy-chained?

YES	**NO**
↓	Go to step 14.

13

Verify the hubs are correctly daisy-chained (Figure 19).

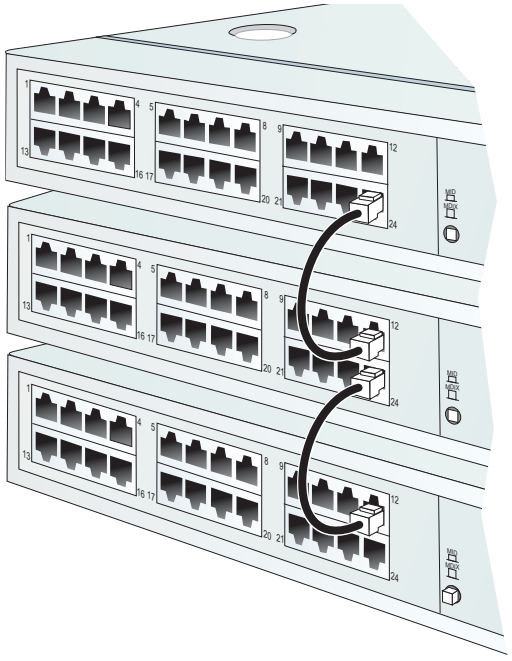


Figure 19: Daisy-Chained Ethernet Hubs

1. At the first (top) Ethernet hub, ensure an RJ-45 Ethernet patch cable connects to port **24** and the medium-dependent interface (MDI) switch is set to **MDI** (in).
2. At the middle Ethernet hub, ensure the patch cable from the top hub connects to port **12,** the patch cable from the bottom hub connects to port **24**, and the MDI switch is set to **MDI** (in).
3. At the bottom Ethernet hub, ensure the patch cable from the middle hub connects to port **12** and the MDI switch is set to **MDIX** (out).

To check two hubs, use step 2 and step 3 (middle and bottom hub instructions only).

Was a corrective action performed?

NO	**YES**
↓	Go to step 1.

14

Verify operation of the Ethernet hub or hubs. Inspect each hub for indications of being powered on, such as:

- Green **Power** LED illuminated.
- Green **Status** LEDs illuminated.

Is a hub failure indicated?

YES	NO
↓	Go to step 16.

15

Remove and replace the Ethernet hub. Refer to the supporting documentation shipped with the hub for instructions.

Did hub replacement solve the problem?

NO	YES
↓	The switch-to-HAFM appliance connection is restored and appears operational. Exit MAP.

Contact the next level of support. Exit MAP.

16

A problem with another LAN-attached device is indicated.

- If the problem is associated with another switch or HAFM appliance, go to "MAP 0000: Start MAP" on page 29 to isolate the problem for that device. Exit MAP.
- If the problem is associated with an unrelated device, notify the customer and have the system administrator correct the problem.

Did repair of an unrelated LAN-attached device solve the problem?

NO	YES
↓	The switch-to-HAFM appliance connection is restored and appears operational. Exit MAP.

17

The Ethernet adapter on the switch CTP card reset in response to an error. The connection to the HAFM appliance terminated briefly, then recovered upon reset.

Perform the data collection procedure and return the CD to HP for analysis. Exit MAP.

18

A protocol mismatch occurred because HAFM and the switch firmware are not at compatible release levels. Recommend to the customer that the downlevel version (software or firmware) be upgraded.

Does HAFM require upgrade?

YES	NO
↓	Go to step 20.

19

Upgrade HAFM. Refer to “Install or Upgrade Software” on page 175.

Did the switch-to-HAFM appliance Ethernet connection recover?

NO	YES
↓	The switch-to-HAFM appliance connection is restored and appears operational. Exit MAP.

Contact the next level of support. Exit MAP.

20

A switch firmware upgrade is required. Refer to “Block and Unblock Ports” on page 161. Perform the data collection procedure after the upgrade.

Did the switch-to-HAFM appliance Ethernet connection recover?

NO	YES
↓	The switch-to-HAFM appliance connection is restored and appears operational. Exit MAP.

Contact the next level of support. Exit MAP.

21

An instance of the HAFM is open at another HAFM appliance and is communicating with the switch (duplicate session). Notify the customer and either:

- Power off the HAFM appliance running the second instance of the application, or

- Configure the HAFM appliance running the second instance of the application as a client workstation.

Does the customer want the second HAFM appliance configured as a client?

YES	NO
↓	Power off the HAFM appliance reporting the **Duplicate Session** communication problem. Exit MAP.

22

Determine the internet protocol (IP) address of the HAFM appliance running the first instance of HAFM.

1. After the HAFM appliance powers on and successfully completes POSTs, the LCD panel displays a `Welcome!!` message, then continuously cycles through and displays the following operational information:
   - Host name.
   - System date and time.
   - LAN 1 and LAN 2 IP addresses.
   - Fan rotational speed.
   - CPU temperature.
   - Hard disk capacity.
   - Virtual and physical memory capacity.
2. After a few seconds, the LCD panel displays the following (Figure 20):

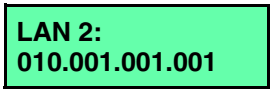


Figure 20: LCD panel (LAN 2 IP address)

3. Depending on switch-to-HAFM appliance LAN connectivity, record the appropriate IP address (LAN 1 or LAN 2).

Continue to the next step.

23

Configure the HAFM appliance reporting the `Duplicate Session` communication problem as a client.

1. At the HAFM main window, click **SAN > Logout**. The application logs out and the HAFM Login dialog box displays.
2. Type a user ID and password (obtained in "MAP 0000: Start MAP" on page 29, and both are case sensitive).
3. Type the IP address of the HAFM appliance running the first instance of HAFM in the **Network Address** field.
4. Click **Login**. HAFM opens and the HAFM main window displays.

Did the HAFM appliance reconfigure as a client and did the Ethernet connection recover?

NO	YES
↓	The switch-to-HAFM appliance connection is restored and the second HAFM appliance appears operational as a client. Exit MAP.

Contact the next level of support. Exit MAP.

24

The IP address defining the switch to HAFM is incorrect or unknown and must be verified. A maintenance terminal (PC) and asynchronous RS-232 null modem cable are required to verify the switch IP address. The tools are provided with the switch or by service personnel. To verify the IP address:

1. Remove the protective cap from the 9-pin maintenance port at the rear of the switch (a phillips screwdriver may be required). Connect one end of the RS-232 null modem cable to the port.
2. Connect the other cable end to a 9-pin communication port (**COM1** or **COM2**) at the rear of the maintenance terminal PC.
3. Power on the maintenance terminal. After the PC powers on, the Windows desktop displays.
4. At the Windows desktop, click **Start** at the left side of the task bar. The **Windows Workstation** menu displays.

Note: The following steps describe inspecting the IP address using *HyperTerminal* serial communication software.

5. At the **Windows Workstation** menu, click **Programs > Accessories > Communications > HyperTerminal**. The Connection Description dialog box displays
6. Type **Edge Switch 2/32** in the **Name** field and click **OK**. The Connect To dialog box displays.
7. Ensure the **Connect using** field displays **COM1** or **COM2** (depending on the serial communication port connection to the switch), and click **OK**. The COM*n* dialog box displays, where *n* is **1** or **2**.
8. Configure the **Port Settings** parameters as follows:
   - **Bits per second–115200**.
   - **Data bits–8**.
   - **Parity–None**.
   - **Stop bits–1**.
   - **Flow control–Hardware** or **None**.

   When the parameters are set, click **OK**. The Edge Switch 2/32 - HyperTerminal dialog box displays.
9. At the **>** prompt, type the user-level password (default is `password`) and press **Enter**. The password is case sensitive. The Edge Switch 2/32 - HyperTerminal dialog box displays with a **C>** prompt at the bottom of the window.
10. At the `C>` prompt, type `ipconfig` and press **Enter**. The Edge Switch 2/32 - HyperTerminal dialog box displays with configuration information listed, including the IP address.
11. Record the switch IP address.
12. Click **Exit** from the **File** pull-down menu to close the HyperTerminal application. A HyperTerminal dialog box displays.
13. Click **Yes**. A second HyperTerminal dialog box displays.
14. Click **No** to exit and close the *HyperTerminal* application.
15. Power off the maintenance terminal.

16. Disconnect the RS-232 null modem cable from the switch and the maintenance terminal. Replace the protective cap over the maintenance port.

Continue to the next step.

25

Define the switch's correct IP address (determined in step 24) to the HAFM appliance.

1. From the HAFM main window, click **Discover > Setup**. The Discover Setup dialog box displays (Figure 21).

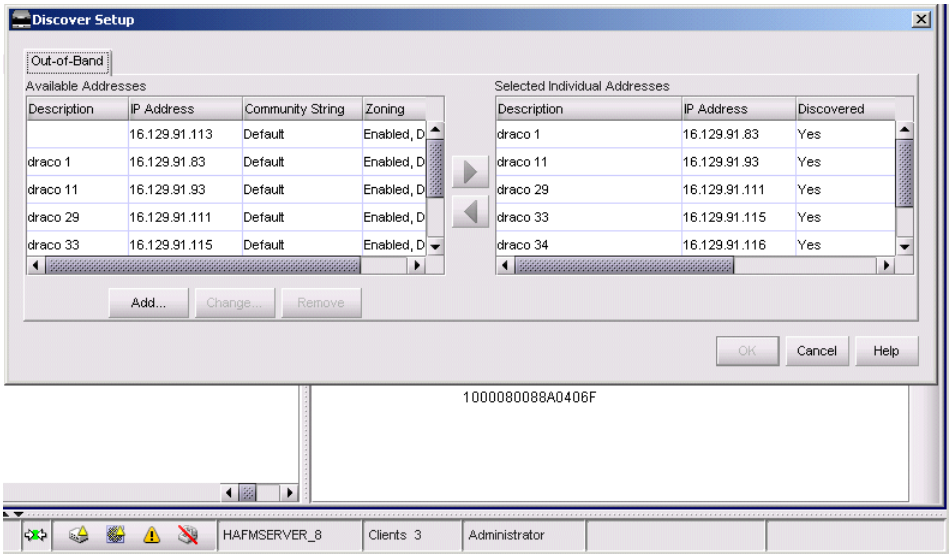


Figure 21: Discover Setup dialog box

2. At the **Available Addresses** field, select (highlight) the switch to be reconfigured and click **Change**. The Editing Domain Information dialog box displays (Figure 22).

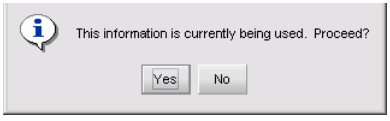


Figure 22: Editing Domain Information dialog box

3. Click **Yes**. The Domain Information dialog box displays with the **IP Address** page open by default (Figure 23).

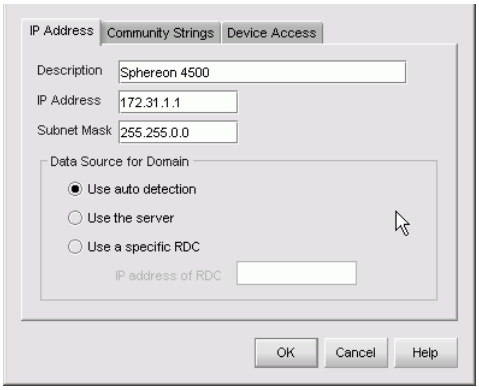


Figure 23: Domain Information dialog box (IP Address page)

4. Type the correct switch IP address in the **IP Address** field.
5. Click **OK** to save the new IP address, close the dialog box, and redefine the switch to HAFM.
6. Click **OK** to close the Discover Setup dialog box and return to HAFM.

At HAFM master log, did the IP address associated with the switch change to the new entry and did the Ethernet connection recover?

NO	**YES**
↓	The switch-to-HAFM appliance connection is restored and appears operational. Exit MAP.

Contact the next level of support. Exit MAP.

26

An incorrect product type is defined to the HAFM appliance.

1. Right-click the product icon with a grey square and yellow exclamation mark (representing the switch reporting the problem) at HAFM's physical map. A pop-up menu appears.
2. Click the **Delete** option from the pop-up menu. The HAFM Message dialog box displays (Figure 24).

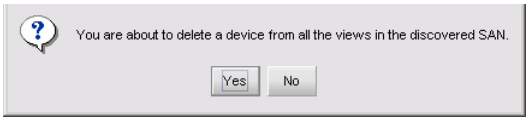


Figure 24: HAFM Message dialog box

3. Click **Yes** to delete the switch.
4. At the HAFM main window, click **Discover** > **Setup**. The Discover Setup dialog box displays.
5. Click **Add**. The Domain Information dialog box displays with the **IP Address** page open by default (Figure 23).
6. Type a switch description in the **Description** field.
7. Type the switch IP address (determined by the customer's network administrator) in the **IP Address** field.
8. Type the switch subnet mask (determined by the customer's network administrator) in the **Subnet Mask** field.
9. At the **Data Source for Domain** area of the dialog box, click the **Use auto detection**, **Use the server**, or **Use a specific RDC** radio button (determined by the customer's network administrator).
10. Click **OK** to save the entered information, close the dialog box, and define the new product configuration to HAFM.
11. Click **OK** to close the Discover Setup dialog box and return to HAFM.

At the HAFM master log, did the IP address associated with the switch change to the new product configuration and did the Ethernet connection recover?

NO	**YES**
↓	The switch-to-HAFM appliance connection is restored and appears operational. Exit MAP.

Contact the next level of support. Exit MAP.

MAP 0500: FRU Failure Analysis

"MAP 0000: Start MAP" on page 29This MAP describes fault isolation for the CTP (which is not an FRU) and fan FRUs. Failure indicators include:

- The amber LED on a fan illuminates.
- The amber emulated LED on a fan graphic at the **Hardware View** illuminates.
- A blinking red and yellow diamond (failed FRU indicator) displays at the **Hardware View**.
- An event code recorded at the switch **Event Log** or the **Embedded Web Server Event Log**.
- A `Failed` or `Not Installed` message associated with a fan at the Embedded Web Server interface.

1

Was an event code **300**, **301**, **302**, **303**, **304**, **305**, **306**, **307;** or **604**, **605**, **607**; or **800**, **801**, **802**, **805**, **806**, **807**, **810**, **811**, **812**, or **850** observed at the switch **Event Log** (HAFM appliance) or at the **Embedded Web Server Event Log**?

YES **NO**

↓ Go to step 3.

2

Table 8 lists event codes, brief explanations of the codes, and associated steps that describe fault isolation procedures.

Table 8: MAP 500: Event Codes

Event Code	Explanation	Action
300	First cooling fan failed.	Go to step 8.
301	Second cooling fan failed.	Go to step 8.
302	Third cooling fan failed.	Go to step 8.
303	Fourth cooling fan failed.	Go to step 8.
604	SBAR failure.	Go to step 14.
605	SBAR revision not supported.	Go to step 12.
800	High-temperature warning (port module sensor).	Go to step 8.
801	Critically hot temperature warning (port module thermal sensor).	Go to step 8.

Table 8: MAP 500: Event Codes

Event Code	Explanation	Action
802	Port module shutdown due to thermal violations.	Go to step 8.
805	High-temperature warning (SBAR thermal sensor).	Go to step 8.
806	Critically hot temperature warning (SBAR thermal sensor).	Go to step 8.
807	SBAR shutdown due to thermal violation.	Go to step 8.
810	High temperature warning (CTP thermal sensor).	Go to step 8.
811	Critically hot temperature warning (CTP thermal sensor).	Go to step 8.
812	CTP shutdown due to thermal violation.	Go to step 8.
850	System shutdown due to CTP thermal violations.	Go to step 8.

3

Is remote fault isolation being performed at the switch or HAFM appliance?

YES **NO**

↓ Remote fault isolation is being performed through the Embedded Web Server interface. Go to step 6.

4

Does a blinking red and yellow diamond (failed FRU indicator) overlay a fan (cooling fan assembly) graphic at the **Hardware View**?

NO **YES**

↓ Go to step 8.

5

Does inspection of a fan indicate a failure? Indicators include:

- The amber LED at the upper left corner of a fan illuminates.
- The fan is not rotating.

NO **YES**

↓ Go to step 8.

The switch appears operational. Exit MAP.

6

Does the Embedded Web Server interface appear operational?

YES **NO**

↓ Analysis for an Ethernet link, AC power distribution, or CTP failure is not described in this MAP. Go to "MAP 0000: Start MAP" on page 29. If this is the second time at this step, contact the next level of support.

7

Inspect the fan operational states at the Embedded Web Server interface.

1. At the **View** panel, click the **FRU Properties** tab. The **View** panel (**FRU Properties** tab) displays.
2. Inspect the **Status** fields for Fan 0 through Fan 3.

Does the **Status** field display a `Failed` message for any fan?

YES **NO**

↓ The switch appears operational. Exit MAP.

8

A fan failed or is improperly installed.

1. Partially remove the fan from the chassis.
2. Reseat the fan in the chassis.

Does the fan appear to function?

NO **YES**

↓ The switch appears operational. Exit MAP.

9

A fan failed and must be removed and replaced ("RRP: Cooling Fan" on page 185).

Does the fan appear to function?

NO **YES**

↓ The switch appears operational.

Contact the next level of support. Exit MAP.

10

Have the customer inspect and verify that facility power is within specifications. These specifications are:

- One single-phase connection for each power supply.
- Input power between 120 and 230 Vac.
- Input current between 2 and 4 amps.
- Input frequency between 47 and 63 Hz.

Is facility power within specifications?

YES **NO**

↓ Ask the customer to correct the facility power problem. When facility power is corrected, verify switch temperature cools to within the operational limit.

11

Inspect the fans. Do one or more fans appear to rotate at insufficient angular velocity (failure pending)?

NO **YES**

↓ Remove and replace the affected fan ("RRP: Cooling Fan" on page 185). After fan replacement, verify switch temperature cools to within the operational limit.

A power supply problem is indicated. Go to "MAP 0100: Power Distribution Analysis" on page 51.

12

An SBAR is not recognized by switch firmware because the firmware version is not supported or the SBAR failed. Advise the customer of the problem and determine the correct firmware version to download from the HAFM appliance.

Download the firmware ("Download a Firmware Version to a Switch" on page 167). Perform the procedure described in "Collecting Maintenance Data" on page 151 after the download.

Continue.

13

Did the firmware download solve the problem?

NO **YES**

↓ The switch appears operational.

14

The SBAR on the CTP card failed. Because the SBAR is not a FRU, SBAR failure requires replacing the switch.

Contact the next level of support.

MAP 0600: Port Failure and Link Incident Analysis

This MAP describes fault isolation for shortwave laser small form factor pluggable (SFP) optical transceivers, longwave laser SFP optical transceivers, and Fibre Channel link incidents. Failure indicators include:

- An event code recorded at the EWS Event Log or Edge Switch Event Log (HAFM appliance).
- A link incident event code recorded at the console of an OSI server attached to the switch reporting the problem.
- One or more amber LEDs on the ports illuminate.
- A port operational state message or a `Failed` message associated with a port at the EWS interface.
- One or more emulated amber LEDs on a port graphic at the **Hardware View** illuminate.
- A blinking red and yellow diamond (failed FRU indicator) appears over a port graphic or a yellow triangle (attention indicator) appears at the alert panel of the **Hardware View**.
- A link incident message recorded in the Link Incident Log or Port Properties dialog box.

1

Was an event code **080, 081, 506**, **507**, **512**, or **514** observed at the EWS Event Log or at the Edge Switch Event Log (HAFM appliance)?

NO	**YES**
↓	Go to step 3.

2

Was an event code **581**, **582**, **583**, **584**, **585**, or **586** observed at the console of an OSI server attached to the switch reporting the problem?

YES	**NO**
↓	Go to step 4.

3

Table 9 lists event codes, brief explanations of the codes, and associated steps that describe fault isolation procedures.

Table 9: MAP 600 Event Codes

Event Code	Explanation	Action
080	Unauthorized worldwide name.	Go to step 21.
081	Invalid attachment.	Go to step 22.
506	Fibre Channel port failure.	Go to step 6.
507	Loopback diagnostics port failure.	Go to step 18.
512	SFP optical transceiver nonfatal error.	Go to step 6.
514	SFP optical transceiver failure.	Go to step 6.
581	Implicit incident.	Go to step 34.
582	Bit error threshold exceeded.	Go to step 34.
583	Loss of signal or loss of synchronization.	Go to step 34.
584	Not operational primitive sequence received.	Go to step 34.
585	Primitive sequence timeout.	Go to step 34.
586	Invalid primitive sequence received for current link state.	Go to step 34.

4

Is fault isolation being performed at the switch?

YES **NO**

↓ Fault isolation is being performed at the EWS interface or HAFM appliance. Go to step 7.

5

Each port has an amber LED and a blue (2 Gb/s operation) or green (1 Gb/s operation) LED adjacent to the port. The amber LED illuminates and the blue or green LED extinguishes if the port fails.

Is an amber port LED illuminated but not blinking (beaconing)?

YES **NO**

↓ The switch appears operational, however a link incident or other problem may have occurred. Perform fault isolation at the HAFM appliance. Go to step 13.

6

As indicated by a message or event code **506**, **512**, or **514**, a Fibre Channel port failed and the SFP optical transceiver must be removed and replaced. Refer to "RRP: SFP Optical Transceiver" on page 181.

- This procedure is concurrent and can be performed while the switch is powered on and operational.
- Verify location of the failed port.
- Replace the optical transceiver with a transceiver of the same type (shortwave or longwave).
- Perform an external loopback test for the port as part of FRU removal and replacement. Refer to "Perform Loopback Tests" on page 146.

Did optical transceiver replacement solve the problem?

NO	**YES**
↓	The switch appears operational. Exit MAP.

Contact the next level of support. Exit MAP.

7

Is fault isolation being performed at the EWS interface?

YES	**NO**
↓	Fault isolation is being performed at the HAFM appliance. Go to step 13.

8

Does the EWS interface appear operational?

NO	**YES**
↓	Go to step 11.

9

A `Page cannot be found, Unable to locate the server, HTTP 404 - file not found`, or other similar message appears. The message indicates the PC cannot communicate with the switch because:

- The switch-to-PC Internet link could not be established.
- AC power distribution in the switch failed, or AC power was disconnected.

- The switch CTP card failed.

Continue to the next step.

10

Ensure the switch is connected to facility AC power. Inspect the switch for indications of being powered on, such as:

- At the front bezel, an illuminated **PWR** LED (green) or **ERR** LED (amber).
- Illuminated LEDs adjacent to Fibre Channel ports.
- Audio emanations and airflow from cooling fans.

Does the switch appear powered on?

YES	NO
↓	Analysis for an Ethernet link, AC power distribution, or CTP failure is not described in this MAP. Go to "MAP 0000: Start MAP" on page 29. If this is the second time at this step, contact the next level of support. Exit MAP.

11

Inspect Fibre Channel port operational states at the EWS interface.

1. At the **View** panel, click the **Port Properties** tab. The **View** panel (**Port Properties** tab) displays with port **0** highlighted in red.
2. Click the port number (**0** through **31**) for which a failure is suspected to display properties for that port.
3. Inspect the **Operational State** field. Scroll down the **View** panel as necessary.
4. Table 10 lists port operational states and MAP 0600 steps that describe fault isolation procedures.

Table 10: Port Operational States and Actions (EWS)

Operational State	Action
Offline	Go to step 19.
Not Operational	Go to step 19.
Port Failure	Go to step 6.
Testing	Internal or external loopback test in process. Exit MAP.

Table 10: Port Operational States and Actions (EWS) (Continued)

Operational State	Action
Invalid Attachment	Go to step 22.
Link Reset	Go to step 33.
Not Installed	Go to step 12.

12

Install an SFP optical transceiver in the port receptacle. Refer to "RRP: SFP Optical Transceiver" on page 181.

- This procedure is concurrent and can be performed while the switch is powered on and operational.
- Verify location of the failed port.
- Perform an external loopback test for the port as part of FRU removal and replacement. Refer to "Perform Loopback Tests" on page 146.

Exit MAP.

13

At the HAFM appliance, does a blinking red and yellow diamond (failed FRU indicator) appear adjacent to a Fibre Channel port graphic at the **Hardware View**?

NO **YES**

↓ A port failure is indicated. Go to step 6.

14

Did a Fibre Channel port fail a loopback test?

NO **YES**

↓ Go to step 18.

15

Does a yellow triangle (attention indicator) appear adjacent to a port graphic at the **Hardware View**?

YES **NO**

↓ Go to step 17.

16

Inspect the port state and LED status for all ports with an attention indicator.

1. At the **Hardware View**, double-click the port graphic with the attention indicator. The Port Properties dialog box displays.
2. Inspect the **Operational State** field at the Port Properties dialog box, and the emulated green and amber LEDs adjacent to the port at the **Hardware View**.
3. Table 11 lists LED and port operational state combinations and associated MAP 0600 (or other) steps that describe fault isolation procedures.

Table 11: Port Operational and LED States (HAFM appliance)

Operational State	Green LED	Amber LED	Action
Offline	Off	Off	Go to step 19.
Not Operational	Off	Off	Go to step 19.
Testing	Off	Blinking	Internal loopback test in process. Exit MAP.
Testing	On	Blinking	External loopback test in process. Exit MAP.
Beaconing	Off or On	Blinking	Go to step 20.
Invalid Attachment	On	Off	Go to step 22.
Link Reset	Off	Off	Go to step 33.
Link Incident	Off	Off	Go to step 34.
Segmented E_Port	On	Off	Go to MAP 0700: Fabric, ISL, and Segmented Port Problem Determination.

17

A link incident may have occurred, but the LIN alerts option is not enabled for the port and the attention indicator does not appear.

At the **Hardware View**, click **Logs > Link Incident Log**. The Link Incident Log displays. If a link incident occurred, the affected port number is listed with one of the following messages.

- `Link interface incident - implicit incident`
- `Link interface incident - bit-error threshold exceeded`

- `Link failure - loss of signal or loss of synchronization`
- `Link failure - not-operational primitive sequence (NOS) received`
- `Link failure - primitive sequence timeout`
- `Link failure - invalid primitive sequence received for the current link state`

Did one of the listed messages appear in the Link Incident Log?

YES	NO
↓	The switch appears operational. Exit MAP.

Go to step 34.

18

As indicated by a message or event code **507**, a Fibre Channel port failed an internal or external loopback test.

1. Reset each port that failed the loopback test.
   a. At the **Hardware View**, right-click the port. A pop-up menu appears.
   b. Click **Reset Port**. A `This operation will cause a link reset to be sent to the attached device` message displays.
   c. Click **OK**. The port resets.
2. Perform an external loopback test for all ports that were reset. Refer to "Perform Loopback Tests" on page 146.

Did resetting ports solve the problem?

NO	YES
↓	The switch appears operational. Exit MAP.

19

A switch port is unblocked and receiving the offline sequence (OLS) or not operational sequence (**NOS**) from an attached device.

Inform the customer that the attached device failed or is set offline, and to take the appropriate corrective action. Exit MAP.

20

Beaconing is enabled for the port.

1. Consult the customer and next level of support to determine the reason port beaconing is enabled.
2. Disable port beaconing.
   a. At the **Hardware View**, right-click the port graphic. A pop-up menu appears.
   b. Click the **Enable Beaconing** option. The check mark disappears from the box adjacent to the option, and port beaconing is disabled.

Was port beaconing enabled because port failure or degradation was suspected?

YES **NO**

↓ The switch appears operational. Exit MAP.

Go to step 1.

21

As indicated by a message or event code **080**, the eight-byte (16-digit) worldwide name (WWN) entered to configure port binding is not valid or a nickname was used that is not configured for the attached device in the *Element Manager* application.

From the **Hardware View**, click **Node List**. Note the **Port WWN** column. This is the WWN assigned to the port or Fibre Channel interface installed on the attached device.

- If a nickname is not assigned to the WWN, the WWN is prefixed by the device manufacturer's name.
- If a nickname is assigned to the WWN, the nickname appears in place of the WWN.

The bound WWN must be entered in the form of a raw WWN format (`XX:XX:XX:XX:XX:XX:XX:XX`) or must be a valid nickname. Ensure a valid WWN or nickname is entered.

Did configuring the WWN or nickname solve the problem?

NO **YES**

↓ The switch appears operational. Exit MAP.

Contact the next level of support. Exit MAP.

22

As indicated by a message or event code **081**, a port has an invalid attachment. The information in the Port Properties dialog box specifies the reason as listed in Table 12.

Table 12: Invalid Attachment Reasons and Actions

Reason	Action
Unknown	Contact the next level of support.
ISL connection not allowed.	Go to step 23.
Incompatible switch.	Go to step 24.
External loopback plug connected.	Go to step 25.
N-Port connection not allowed.	Go to step 23.
Non-HP switch at other end.	Go to step 24.
Unauthorized port binding WWN.	Go to step 21.
Unresponsive node.	Go to step 27.
ESA security mismatch.	Go to step 29.
Fabric binding mismatch.	Go to step 30.
Authorization failure reject.	Go to step 27.
Unauthorized switch binding WWN.	Go to step 31.
Fabric mode mismatch.	Go to step 24.
CNT WAN extension mode mismatch.	Go to step 32.

23

The port connection conflicts with the configured port type and an ISL connection is not allowed. Either an expansion port (E_Port) is incorrectly cabled to a Fibre Channel device or a fabric port (F_Port) is incorrectly cabled to a fabric element.

1. At the HAFM appliance's **Hardware View**, click **Configure > Ports**. The Configure Ports dialog box displays.
2. Use the vertical scroll bar as necessary to display the information row for the port indicating an invalid attachment.
3. Click the **Type** field and configure the port from the list box as follows:
   - Click fabric port (**F_Port**) if the port is cabled to a device (node).

- Click expansion port (**E_Port**) if the port is cabled to a fabric element (director or switch) to form an ISL.

4. Click **Activate** to save the configuration information and close the window.

Did reconfiguring the port type solve the problem?

NO	YES
↓	The switch appears operational. Exit MAP.

Contact the next level of support. Exit MAP.

24

One of the following mode-mismatch conditions was detected and an ISL connection is not allowed:

- The switch is configured for operation in **Open Fabric 1.0** mode and is connected to a fabric element not configured to **Open Fabric 1.0** mode.
- The switch is configured for operation in **Open Fabric 1.0** mode and is connected to a legacy HP switch at the incorrect Exchange Link Parameter (ELP) revision level.
- The switch is configured for operation in **Open Fabric 1.0** mode and is connected to a non-HP switch at the incorrect ELP revision level.
- The switch is configured for operation in **Open Fabric 1.0** mode and is connected to a non-HP switch.

Reconfigure the switch operating mode:

1. Ensure the switch is set offline. Refer to "Set the Switch Online or Offline" on page 159.
2. At the **Hardware View**, click **Configure > Operating Parameters > Fabric Parameters**. The Configure Fabric Parameters dialog box displays (Figure 25).

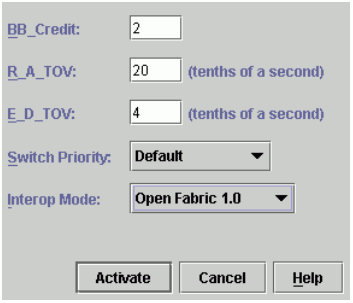


Figure 25: Configure Fabric Parameters dialog box

3. Choose the operating mode as follows:
   - Choose **Open Fabric 1.0** from the **Interop Mode** list box.
   - Choose **Homogeneous** from the **Interop Mode** list box.
4. Click **Activate** to save the selection and close the window.

Did configuring the operating mode solve the problem?

NO	**YES**
↓	The switch appears operational. Exit MAP.

Contact the next level of support. Exit MAP.

25

A loopback (wrap) plug appears to be connected to the port and there is no diagnostic test running. Is a loopback plug in the port receptacle?

YES	**NO**
↓	Contact the next level of support. Exit MAP.

26

Remove the loopback plug from the port receptacle. If directed by the customer, connect a fiber-optic cable attaching a device to the switch.

- If the port is operational and a device is not attached, both LEDs adjacent to the port extinguish and the port state is **No Light**.
- If the port is operational and a device is attached, the blue or green LED illuminates, the amber LED extinguishes, and the port state is **Online**.

Did removing the loopback plug solve the problem?

NO	**YES**
↓	The switch appears operational. Exit MAP.

Contact the next level of support. Exit MAP.

27

A port connection timed out because of an unresponsive device (node) or an ISL connection was not allowed because of a security violation (authorization failure reject). Check the port status and clean the fiber-optic connectors on the cable.

1. Notify the customer the port will be blocked. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port and sets the attached device offline.
2. Block the port. Refer to "Clean Fiber-Optic Components" on page 153.
3. Disconnect both ends of the fiber-optic cable.
4. Clean the fiber-optic connectors. Refer to "IML, IPL, or Reset the Switch" on page 156.
5. Reconnect the fiber-optic cable.
6. Unblock the port. Refer to "Clean Fiber-Optic Components" on page 153.
7. Monitor port operation for approximately five minutes.

Is the invalid attachment problem solved?

YES	NO
↓	The Fibre Channel link and switch appear operational. Exit MAP.

28

Inspect and service the host bus adapters (HBAs) as necessary.

Did service of the HBAs solve the problem?

NO	YES
↓	Exit MAP.

Contact the next level of support. Exit MAP.

29

A port connection is not allowed because of an Exchange Security Attribute (ESA) feature mismatch. Switch binding parameters must be compatible for both fabric elements.

1. At the **Hardware View** for each switch, click **Configure > Switch Binding > Change State**. The Switch Binding - State Change dialog box displays (Figure 26).

Figure 26: Switch Binding - State Change dialog box

2. Ensure the **Enable Switch Binding** check box is enabled (checked) for both switches.
3. Ensure the **Connection Policy** radio buttons are compatible for both switches.
4. Click **Activate** for each switch. The switch binding feature is consistently enabled for both switches.

Did configuring the switch binding parameters solve the problem?

NO **YES**

↓ The switch appears operational. Exit MAP.

Contact the next level of support. Exit MAP.

30

A port connection is not allowed because of a fabric binding mismatch. Fabric membership lists must be compatible for both fabric elements.

1. At the HAFM main window, click Configure > **Fabric Binding**. The Fabric Binding dialog box displays (Figure 27).

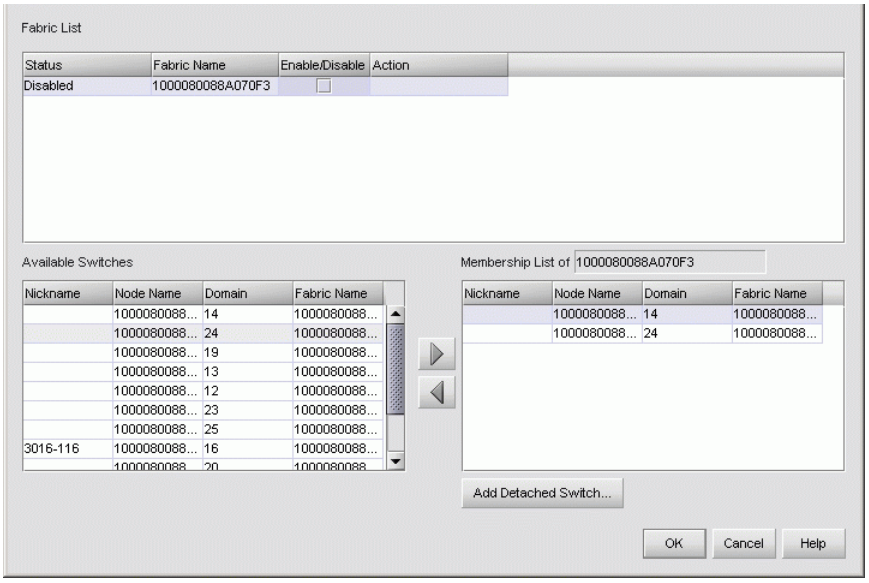


Figure 27: Fabric Binding dialog box

2. At the **Fabric List** section, ensure the **Enable/Disable** check box is enabled (checked) for the fabric containing both switches.
3. At the **Membership List of <Fabric Name>** section, update the membership list for both elements to ensure interswitch compatibility, then click **OK**. The fabric binding feature is consistently enabled for both switches.

Did updating the fabric membership lists solve the problem?

NO **YES**

↓ The switch appears operational. Exit MAP.

Contact the next level of support. Exit MAP.

31

A port connection is not allowed because of a switch binding mismatch. Switch membership lists must be compatible for both fabric elements.

1. At the **Hardware View** for each switch, click **Configure > Switch Binding > Edit Membership List**. The Switch Binding - Membership List dialog box displays (Figure 28).

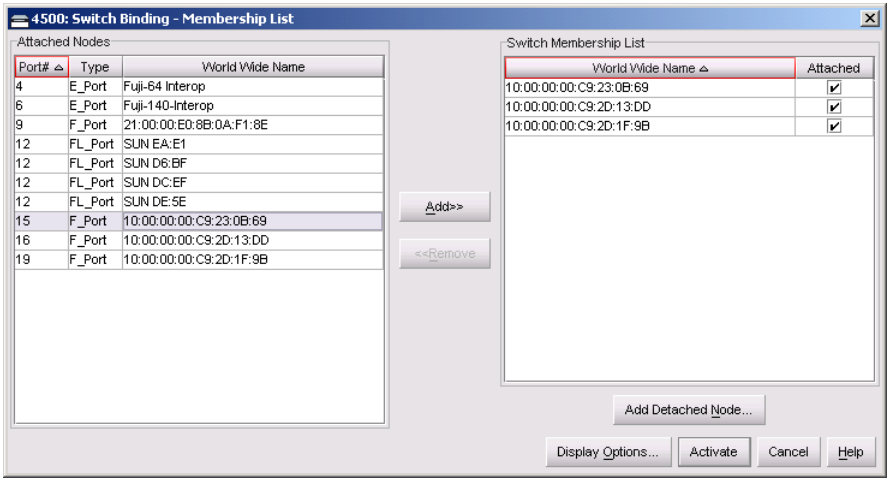


Figure 28: Switch Binding - Membership List dialog box

2. At the Switch Binding - Membership List dialog box ensure the **Switch Membership List** is updated and correct for each switch, then click **Activate** for each switch. The switch binding feature is consistently enabled for both switches.

Did updating the switch membership lists solve the problem?

NO	**YES**
↓	The switch appears operational. Exit MAP.

Contact the next level of support. Exit MAP.

32

A port connection is not allowed because of a Computer Network Technologies (CNT) wide area network (WAN) extension mode mismatch. Based on switch-to-switch differences between the ELP maximum frame sizes allowed, a connection was not allowed to a switch set to CNT WAN extension mode.

Contact HP support personnel to obtain software maintenance release 4.02.00. This release is required to correct the problem and allow HP switches to communicate with CNT UltraEdge WAN Gateways. Exit MAP.

33

The switch and attached device are performing a Fibre Channel link reset. This is a transient state. Wait approximately 30 seconds and inspect port state and LED behavior.

Did the link recover and resume operation?

NO	YES
↓	The Fibre Channel link and switch appear operational. Exit MAP.

Go to step 1.

34

A link incident message appeared in the Link Incident Log or in the **Link Incident** field of the Port Properties dialog box; or an event code 581, 582, 583, 584, 585, or 586 was observed at the console of an OSI server attached to the switch reporting the problem.

Clear the link incident for the port.

1. At the **Hardware View**, right-click the port. A pop-up menu appears.
2. Click **Clear Link Incident Alert(s)**. The Clear Link Incident Alert(s) dialog box displays (Figure 29).

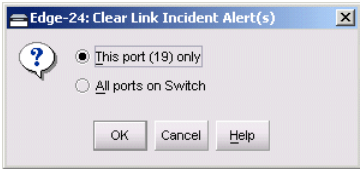


Figure 29: Clear Link Incident Alert(s) dialog box

3. Click the **This port (*n*) only** radio button (where ***n*** is the port number) and click **OK**. The link incident clears.
4. Monitor port operation for approximately five minutes.

Did the link incident recur?

YES	NO
↓	The problem is transient and the Fibre Channel link and switch appear operational. Exit MAP.

35

Inspect the fiber-optic jumper cable attached to the port and ensure the cable is not bent and connectors are not damaged. If the cable is bent or connectors are damaged:

1. Notify the customer the port will be blocked. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port and sets the attached device offline.
2. Block the port. Refer to "Clean Fiber-Optic Components" on page 153.
3. Remove and replace the fiber-optic jumper cable.
4. Unblock the port. Refer to "Clean Fiber-Optic Components" on page 153.

Was a corrective action performed?

YES	NO
↓	Go to step 37.

36

Monitor port operation for approximately five minutes.

Did the link incident recur?

YES	NO
↓	The Fibre Channel link and switch appear operational. Exit MAP.

37

Clean fiber-optic connectors on the jumper cable.

1. Notify the customer the port will be blocked. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port and sets the attached device offline.
2. Block the port. Refer to "Clean Fiber-Optic Components" on page 153.
3. Disconnect both ends of the fiber-optic cable.
4. Clean the fiber-optic connectors. Refer to "IML, IPL, or Reset the Switch" on page 156.
5. Reconnect the fiber-optic cable.
6. Unblock the port. Refer to "Clean Fiber-Optic Components" on page 153.
7. Monitor port operation for approximately five minutes.

Did the link incident recur?

YES	NO
↓	The Fibre Channel link and switch appear operational. Exit MAP.

38

Disconnect the fiber-optic jumper cable from the switch port and connect the cable to a spare port.

Is a link incident reported at the new port?

YES	NO
↓	Go to step 40.

39

The attached device is causing the recurrent link incident. Notify the customer of the problem and have the system administrator:

1. Inspect and verify operation of the attached device.
2. Repair the attached device if a failure is indicated.
3. Monitor port operation for approximately five minutes.

Did the link incident recur?

YES	NO
↓	The attached device, Fibre Channel link, and switch appear operational. Exit MAP.

Contact the next level of support. Exit MAP.

40

The switch port reporting the problem is causing the recurrent link incident. The recurring link incident indicates port degradation and a possible pending failure. Go to step 6.

MAP 0700: Fabric, ISL, and Segmented Port Problem Determination

This MAP describes isolation of fabric logout, interswitch link (ISL), and E_Port segmentation problems. Failure indicators include:

- An event code recorded at the EWS Event Log or Edge Switch Event Log (HAFM appliance).
- A segmentation reason associated with a Fibre Channel port at the EWS interface.
- A yellow triangle (attention indicator) appears adjacent to a port graphic at the alert panel of the **Hardware View**.
- A link incident message recorded in the Link Incident Log or Port Properties dialog box.

1

Was an event code **011**, **021**, **051**, **052**, **061**, **062**, **063**, **070**, **071**, **072**, **140**, **142**, or **150** observed at the EWS Event Log or at the Edge Switch Event Log (HAFM appliance)?

YES	NO
↓	Go to step 3.

2

Table 13 lists event codes, brief explanations of the codes, and associated steps that describe fault isolation procedures.

Table 13: MAP 700 Event Codes

Event Code	Explanation	Action
011	Login Server database invalid.	Go to step 9.
021	Name Server database invalid.	Go to step 9.
051	Management Server database invalid.	Go to step 10.
052	Management Server internal error.	Go to step 10.
061	Fabric Controller database invalid.	Go to step 11.
062	Maximum interswitch hop count exceeded.	Go to step 12.
063	Remote switch has too many ISLs.	Go to step 13.
070	E_Port is segmented.	Go to step 14.

Table 13: MAP 700 Event Codes (Continued)

Event Code	Explanation	Action
071	Switch is isolated.	Go to step 14.
072	E_Port connected to unsupported switch.	Go to step 22.
140	Congestion detected on an ISL.	Go to step 23.
142	Low BB_Credit detected on an ISL.	Go to step 24.
150	Zone merge failure.	Go to step 25.

3

Is fault isolation being performed through the EWS interface?

YES **NO**

↓ Fault isolation is being performed at the HAFM appliance. Go to step 6.

4

Does the EWS interface appear operational?

YES **NO**

↓ Analysis for an Ethernet link, AC power distribution, or CTP failure is not described in this MAP. Go to "MAP 0000: Start MAP" on page 29. If this is the second time at this step, contact the next level of support. Exit MAP.

5

Inspect the Fibre Channel port segmentation reason at the EWS interface.

1. At the **View** panel, click the **Port Properties** tab. The **View** panel (**Port Properties** tab) displays.
2. Click the port number (**0** through **31**) of the segmented port.
3. Inspect the **Reason** field for the selected port.

Is the **Reason** field blank or does it display an `N/A` message?

NO **YES**

↓ The switch ISL appears operational. Exit MAP.

The **Reason** field displays a segmentation reason message. Table 14 lists the reasons and associated steps that describe fault isolation procedures.

Table 14: Port Segmentation Reasons and Actions (EWS)

Segmentation Reason	Action
Incompatible operating parameters.	Go to step 15.
Duplicate domain ID.	Go to step 16.
Incompatible zoning configurations.	Go to step 17.
Build fabric protocol error.	Go to step 18.
No principal switch.	Go to step 20.
No response from attached switch (hello timeout).	Go to step 21.

6

At the HAFM appliance, does a yellow triangle (attention indicator) appear adjacent to a Fibre Channel port graphic at the **Hardware View**?

YES **NO**

↓ The problem is transient and the switch-to-fabric element connection appears operational. Exit MAP.

7

Inspect the port state and LED status for all ports with an attention indicator.

1. At the **Hardware View**, double-click the port graphic with the attention indicator. The Port Properties dialog box displays.
2. Inspect the **Operational State** field at the Port Properties dialog box.

Does the **Operational State** field indicate **Segmented E_Port**?

YES **NO**

↓ Analysis for other port or link incident problems is not described in this MAP. Go to "MAP 0600: Port Failure and Link Incident Analysis" on page 89. Exit MAP.

8

Inspect the **Reason** field at the Port Properties dialog box. Table 15 lists port segmentation reasons and associated steps that describe fault isolation procedures.

Table 15: Port Segmentation Reasons and Actions (HAFM Appliance)

Segmentation Reason	Action
Incompatible operating parameters.	Go to step 15.
Duplicate domain ID.	Go to step 16.
Incompatible zoning configurations.	Go to step 17.
Build fabric protocol error.	Go to step 18.
No principal switch.	Go to step 20.
No response from attached switch (hello timeout).	Go to step 21.

9

A minor error occurred that caused the Fabric Services database to be re-initialized to an empty state. As a result, a disruptive fabric logout and login occurred for all attached devices. The following list explains the error:

- **Event code 011–**The Login Server database failed cyclic redundancy check (CRC) validation.
- **Event code 021–**The Name Server database failed CRC validation.

All attached devices resume operation after fabric login. Perform the data collection procedure and return the CD to HP for analysis. Exit MAP.

10

A minor error occurred that caused the HAFM appliance database to be re-initialized to an empty state. As a result, a disruptive server logout and login occurred for all attached devices. The following list explains the error:

- **Event code 051–**The HAFM appliance database failed CRC validation.
- **Event code 052–**An internal operating error was detected by the HAFM appliance subsystem.

All attached devices resume operation after HAFM appliance login. Perform the data collection procedure and return the CD to HP for analysis. Exit MAP.

11

As indicated by an event code **061**, a minor error occurred that caused the Fabric Controller database to be re-initialized to an empty state and fail CRC validation. As a result, the switch briefly lost interswitch link capability.

All interswitch links resume operation after CTP reset. Perform the data collection procedure and return the CD to HP for analysis. Exit MAP.

12

As indicated by an event code **062**, the Fabric Controller software detected a path to another fabric element (director or switch) in a multiswitch fabric that traverses more than three interswitch links (hops). Fibre Channel frames may persist in the fabric longer than timeout values allow.

Advise the customer of the problem and work with the system administrator to reconfigure the fabric so the path between any two fabric elements does not traverse more than three hops.

Did fabric reconfiguration solve the problem?

NO **YES**

↓ The switch and multiswitch fabric appear operational. Exit MAP.

Contact the next level of support. Exit MAP.

13

As indicated by an event code **063**, the Fabric Controller software detected an:

- Director 2/64 in a multiswitch fabric that has more than 48 ISLs attached.
- Other fabric element (other than an Director 2/140) in a multiswitch fabric that has more than 32 ISLs attached.

Fibre Channel frames may be lost or routed in loops because of potential fabric routing problems. Advise the customer of the problem and work with the system administrator to reconfigure the fabric so that no director or switch elements have more than the proscribed number of ISLs.

Did fabric reconfiguration solve the problem?

NO **YES**

↓ The switch and multiswitch fabric appear operational. Exit MAP.

Contact the next level of support. Exit MAP.

14

A **070** event code indicates an E_Port detected an incompatibility with an attached switch and prevented the switches from forming a multiswitch fabric. A segmented E_port cannot transmit Class 2 or Class 3 Fibre Channel traffic.

A **071** event code indicates the switch is isolated from all switches in a multiswitch fabric, and is accompanied by a **070** event code for each segmented E_Port. The **071** event code is resolved when all **070** events are corrected.

Obtain supplementary event data for each **070** event code.

1. At the **Hardware View**, click **Logs > Event Log**. The Event Log displays.
2. Examine the first five bytes (**0** through **4**) of event data.
3. Byte **0** specifies the switch port number (**00** through **31**) of the segmented E_port. Byte **4** specifies the segmentation reason as specified in Table 16.

Table 16: Byte 4 Segmentation Reasons and Actions

Byte 4	Segmentation Reason	Action
01	Incompatible operating parameters.	Go to step 15.
02	Duplicate domain ID.	Go to step 16.
03	Incompatible zoning configurations.	Go to step 17.
04	Build fabric protocol error.	Go to step 18.
05	No principal switch.	Go to step 20.
06	No response from attached switch (hello timeout).	Go to step 21.

15

A switch E_Port segmented because the error detect time out value (E_D_TOV) or resource allocation time out value (R_A_TOV) is incompatible with the attached fabric element.

1. Contact HP support to determine the recommended E_D_TOV and R_A_TOV values for both switches.
2. Notify the customer both switches will be set offline. Ensure the system administrator quiesces Fibre Channel frame traffic through the switches and sets attached devices offline.
3. Set both switches offline. Refer to “Set the Switch Online or Offline” on page 159.
4. At the **Hardware View** for the first switch reporting the problem, click **Configure > Operating Parameters > Fabric Parameters**. The Configure Fabric Parameters dialog box displays (Figure 30).

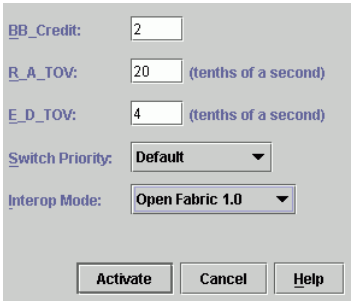


Figure 30: Configure Fabric Parameters dialog box

5. Type the recommended E_D_TOV and R_A_TOV values, then click **Activate**.
6. Repeat steps d and e at the **Hardware View** for the switch attached to the segmented E_Port (second switch). Use the same E_D_TOV and R_A_TOV values.
7. Set both switches online. Refer to "Set the Switch Online or Offline" on page 159.

Did the operating parameter change solve the problem and did both switches join through the ISL to form a fabric?

NO	YES
↓	The switch, associated ISL, and multiswitch fabric appear operational. Exit MAP.

Contact the next level of support. Exit MAP.

16

A switch E_Port segmented because two fabric elements had duplicate domain IDs.

1. Work with the system administrator to determine the desired domain ID (**1** through **31** inclusive) for each switch.
2. Notify the customer both switches will be set offline. Ensure the system administrator quiesces Fibre Channel frame traffic through the switches and sets attached devices offline.
3. Set both switches offline. Refer to "Set the Switch Online or Offline" on page 159.

4. At the **Hardware View** for the first switch reporting the problem, click **Configure > Operating Parameters > Switch Parameters**. The Configure Switch Parameters dialog box displays (Figure 31).

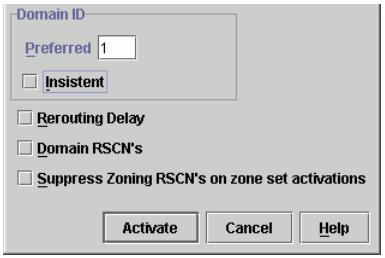


Figure 31: Configure Switch Parameters dialog box

5. Type the customer-determined preferred domain ID value, then click **Activate**.
6. Repeat steps d and e at the **Hardware View** for the switch attached to the segmented E_Port (second switch). Use a different preferred domain ID value.
7. Set both switches online. Refer to "Set the Switch Online or Offline" on page 159.

Did the domain ID change solve the problem and did both switches join through the ISL to form a fabric?

NO	YES
↓	The switch, associated ISL, and multiswitch fabric appear operational. Exit MAP.

Contact the next level of support. Exit MAP.

17

A switch E_Port segmented because two switches had incompatible zoning configurations. An identical zone name is recognized in the active zone set for both switches, but the zones contain different members.

1. Work with the system administrator to determine the desired zone name change for one of the affected switches. Zone names must conform to the following rules:
   - The name must be 64 characters or fewer in length.
   - The first character must be a letter (**a** through **z**), upper or lower case.

— Other characters must be alphanumeric (**a** through **z** or **0** through **9**), dollar sign (**$**), hyphen (**-**), caret (**^**), or underscore (_).

2. Close the *Element Manager* application (**Hardware View**). The HAFM main window (still active) displays.
3. At the HAFM main window physical map, right- click the blue background representing the fabric containing the switch reporting the problem. A pop-up menu appears.
4. Click the **Zoning** option from the menu. The Zoning dialog box displays with the **Zone Library** page open (Figure 32).

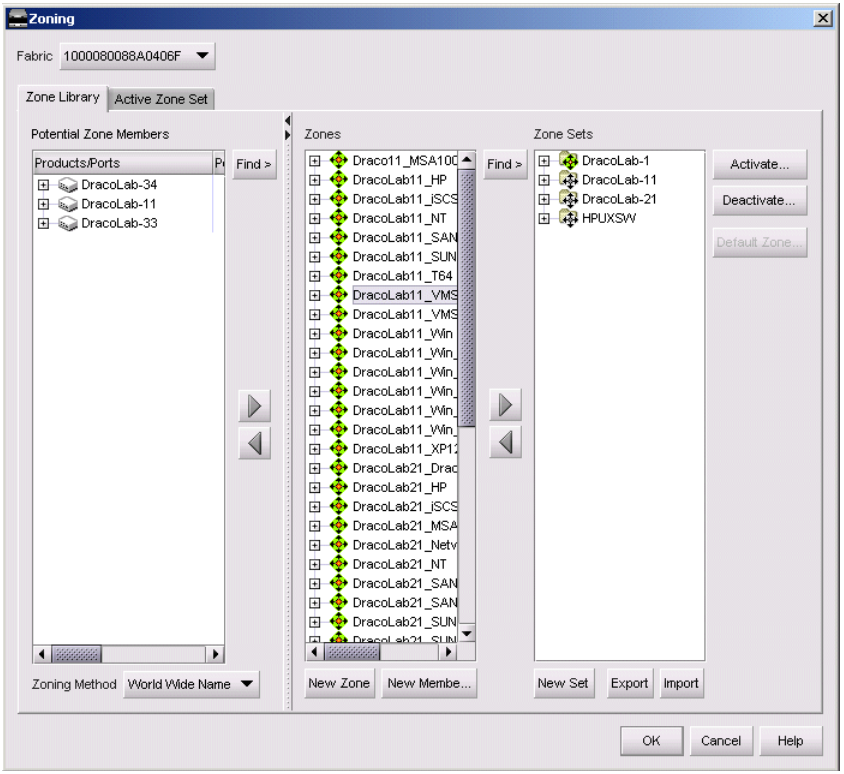


Figure 32: Zoning dialog box (Zone Library tab)

5. Click the **Active Zone Set** tab. The Zoning dialog box displays with the **Active Zone Set** page open (Figure 33).

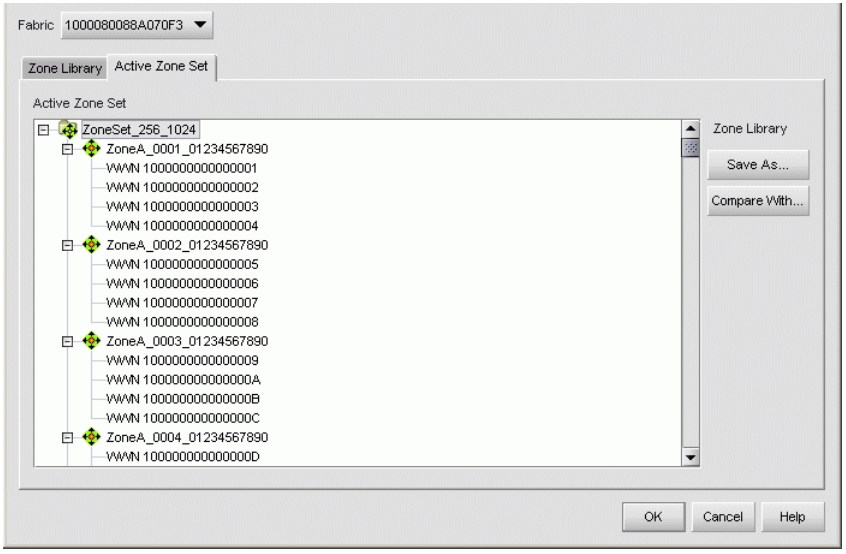


Figure 33: Zoning dialog box (Active Zone Set tab)

6. Inspect zone names in the active zone set to determine the incompatible name.
7. Modify the incompatible zone name as directed by the customer:
   a. At the Zoning dialog box, click the **Zone Library** tab. The dialog box returns to the **Zone Library** page.
   b. At the **Zones** field, right-click the zone name to be changed. A pop-up menu appears.
   c. Click the **Rename** option from the menu. The selected zone name remains highlighted in blue. Type the new zone name (specified by the customer), then click **OK** to activate the change and close the Zoning dialog box.

Did the zone name change solve the problem and did both switches join through the ISL to form a fabric?

NO	**YES**
↓	The switch, associated ISL, and multiswitch fabric appear operational. Exit MAP.

Contact the next level of support. Exit MAP.

18

A switch E_Port segmented because a build fabric protocol error was detected.

1. Disconnect the fiber-optic jumper cable from the segmented E_Port.
2. Reconnect the cable to the same port.

Did disconnecting and reconnecting the cable solve the problem and did both switches join through the ISL to form a fabric?

NO	YES
↓	The switch, associated ISL, and multiswitch fabric appear operational. Exit MAP.

19

Initial program load (IPL) the switch. Refer to "IML, IPL, or Reset the Switch" on page 156.

Did the IPL solve the problem and did both switches join through the ISL to form a fabric?

NO	YES
↓	The switch, associated ISL, and multiswitch fabric appear operational. Exit MAP.

Perform the data collection procedure and contact the next level of support. Exit MAP.

20

A switch E_Port segmented because no switch in the fabric is capable of becoming the principal switch.

1. Notify the customer the switch will be set offline. Ensure the system administrator quiesces Fibre Channel frame traffic through the switch and sets attached devices offline.
2. Set the switch offline. Refer to "Set the Switch Online or Offline" on page 159.
3. At the **Hardware View** for the switch reporting the problem, click **Configure >Operating Parameters > Fabric Parameters**. The Configure Fabric Parameters dialog box displays.

4. At the **Switch Priority** field, click **Principal**, **Never Principal**, or **Default** (the default setting is **Default**). The switch priority value designates the fabric's principal switch. The principal switch is assigned a priority of **1** and controls the allocation and distribution of domain IDs for all fabric switches (including itself).

   Principal is the highest priority setting, **Default** is the next highest, and **Never Principal** is the lowest priority setting. The setting **Never Principal** means that the switch is incapable of becoming a principal switch. If all switches are set to **Principal** or **Default**, the switch with the highest priority and the lowest WWN becomes the principal switch.

   At least one switch in a multiswitch fabric must be set as **Principal** or **Default**. If all switches are set to **Never Principal**, all ISLs segment and the message `No Principal Switch` appears in the **Reason** field of the Port Properties dialog box.

5. Set the switch online. Refer to "Set the Switch Online or Offline" on page 159.

Did the switch priority change solve the problem and did both switches join through the ISL to form a fabric?

NO	YES
↓	The switch, associated ISL, and multiswitch fabric appear operational. Exit MAP.

Contact the next level of support. Exit MAP.

21

A switch E_Port segmented (at an operational switch) because a response (hello timeout) to a verification check indicates an attached switch is not operational.

1. Perform the data collection procedure at the operational switch and return the CD to HP for analysis. This information may assist in fault isolating the failed switch.
2. Go to "MAP 0000: Start MAP" on page 29 and perform fault isolation for the failed switch.

Exit MAP.

22

As indicated by an event code **072**, a switch E_Port is connected to an unsupported switch or fabric element.

Advise the customer of the problem and disconnect the interswitch link to the unsupported switch. Exit MAP.

23

A **140** event code occurs only if the optional OpenTrunking feature is enabled. The event code indicates OpenTrunking firmware detected an ISL with Fibre Channel traffic that exceeds the configured congestion threshold.

No action is required for an isolated event. However, if this event persists, perform one of the following:

- Relieve the congestion by adding parallel ISLs between the switches reporting the problem.
- Increase the ISL link speed between the switches reporting the problem (from 1 Gb/s to 2 Gb/s).
- Reroute Fibre Channel traffic by moving device connections to a less-congested region of the fabric.

Did the corrective action solve the problem and relieve the reported ISL congestion?

NO	**YES**
↓	The ISL appears operational. Exit MAP.

Contact the next level of support. Exit MAP.

24

A **142** event code occurs only if the optional OpenTrunking feature is enabled. The event code indicates OpenTrunking firmware detected an ISL with no transmission BB_Credit for a period of time that exceeded the configured low BB_Credit threshold. This results in downstream fabric congestion.

No action is required for an isolated event or if the reporting ISL approaches 100% throughput. However, if this event persists, perform one of the following:

- Relieve the congestion by adding parallel ISLs between the switches reporting the problem.
- Increase the ISL link speed between the switches reporting the problem (from 1 Gb/s to 2 Gb/s).
- Reroute Fibre Channel traffic by moving device connections to a less-congested region of the fabric.

Did the corrective action solve the problem and relieve the reported low BB_Credit condition?

NO **YES**

↓ The ISL appears operational. Exit MAP.

Contact the next level of support. Exit MAP.

25

A **150** event code indicates a zone merge process failed during ISL initialization. Either an incompatible zone set was detected or a problem occurred during delivery of a zone merge frame. This event code always precedes a **070** event code, and represents the reply of an adjacent fabric element in response to a zone merge frame.

Obtain supplementary event data for each **150** event code.

1. At the **Hardware View**, click **Logs > Event Log**. The Event Log displays.
2. Examine the first 12 bytes (**0** through **11**) of event data.
3. Bytes **0** through **3** specify the E_Port number (**00** through **31**) reporting the problem. Bytes **8** through **11** specify the failure reason as specified in Table 17.

Table 17: Bytes 8 through 11 Failure Reasons and Actions

Bytes 8 - 11	Failure Reason	Action
01	Invalid data length.	Go to step 26.
08	Invalid zone set format.	Go to step 26.
09	Invalid data.	Go to step 27.
0A	Cannot merge.	Go to step 27.
F0	Retry limit reached.	Go to step 26.
F1	Invalid response length.	Go to step 26.
F2	Invalid response code.	Go to step 26.

26

A zone merge process failed during ISL initialization. The following list explains the reason:

- **Failure reason 01–**An invalid data length condition caused an error in a zone merge frame.

- **Failure reason 08–**An invalid zone set format caused an error in a zone merge frame.
- **Failure reason F0–**A retry limit reached condition caused an error in a zone merge frame.
- **Failure reason F1–**An invalid response length condition caused an error in a zone merge frame.
- **Failure reason F2–**An invalid response code caused an error in a zone merge frame.

Disconnect the fiber-optic jumper cable from the E_Port reporting the problem, then reconnect the cable to the same port.

Did disconnecting and reconnecting the cable solve the problem and was the resulting zone merge process successful?

NO **YES**

↓ The merged zone appears operational. Exit MAP.

Perform the data collection procedure and return the CD to HP for analysis. Contact the next level of support. Exit MAP.

27

A zone merge process failed during ISL initialization. The following list explains the reason:

- **Failure reason 09–**Invalid data caused a zone merge failure.
- **Failure reason 0A–**A `Cannot Merge` condition caused a zone merge failure.

Obtain supplementary error code data for the **150** event code.

1. At the **Hardware View**, click **Logs > Event Log**. The Event Log displays.
2. Examine bytes **12** through **15** of event data that specify the error code. Record the error code.

Perform the data collection procedure and return the CD to HP for analysis. Contact the next level of support, and report the **150** event code, the associated failure reason, and the associated error code. Exit MAP.

MAP 0800: HAFM Appliance or Web Browser PC Hardware Problem Determination

This MAP describes isolation of hardware-related problems with the customer-supplied server communicating with the switch through the EWS interface. This MAP also describes isolation of problems related to the HAFM appliance hardware.

The MAP provides high-level fault isolation instructions only. Refer to the documentation provided with the server for detailed problem determination and resolution.

To fault isolate software-related problems with the server, go to "MAP 0300: HAFM Appliance Software Problem Determination" on page 61.

To fault isolate switch-to-server communication problems, go to "MAP 0400: Loss of HAFM Appliance or Web Browser PC Communication" on page 69.

1

Are you performing fault isolation at a customer-supplied server communicating with the switch through the EWS interface?

NO	YES
↓	The server and Internet browser application are not HP-supported and analysis for the failure is not described in this MAP. Refer to the supporting documentation shipped with the server for instructions on resolving the problem. Exit MAP.

2

Are you performing fault isolation at a customer-supplied, Unix-based server running the client SAN management application?

NO	YES
↓	Unix-based servers are not HP-supported and analysis for the failure is not described in this MAP. Refer to the supporting documentation shipped with the server for instructions on resolving the problem. Exit MAP.

3

Are you performing fault isolation at the HAFM appliance running the Windows 2000 Professional operating system?

YES	NO
↓	Analysis for the HAFM appliance failure is not described in this MAP. Contact the next level of support. Exit MAP.

4

At the HAFM appliance, close the *HAFM* application.

1. Click **SAN > Shutdown**. An HAFM Message dialog box displays (Figure 34).

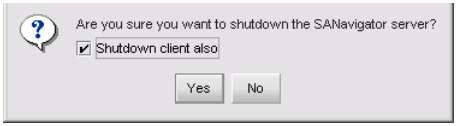


Figure 34: HAFM Message dialog box

2. Click **Yes** to close HAFM.
3. Close any other applications.

Continue to the next step.

5

Inspect the available random access memory (RAM). The HAFM appliance must have a minimum of 128 megabytes (MB) of memory to run the Windows-based operating system and HAFM.

1. Right-click anywhere on the Windows task bar at the bottom of the desktop. A pop-up menu appears.
2. Click **Task Manager**. The Windows Task Manager dialog box displays with the **Applications** page open by default. Click the **Performance** tab to open the **Performance** page.
3. At the **Physical Memory (K)** portion of the dialog box, inspect the total amount of physical memory.
4. Close the dialog box by clicking **Close** (X) at the upper right corner of the window.

Does the HAFM appliance have sufficient memory?

YES	NO
↓	A memory upgrade is required. Inform the customer of the problem and contact the next level of support. Exit MAP.

6

Reboot the HAFM appliance and perform system diagnostics.

1. At the Windows 2000 desktop, click **Start** at the left side of the task bar (bottom of the desktop), then click **Shut Down**. The Shut Down Windows dialog box displays.
2. Click the **Shut Down** option from the list box and click **OK**. The HAFM appliance powers down.
3. Wait approximately 30 seconds and press the power (⏻) button on the LCD panel to power on the HAFM appliance and perform POSTs. During POSTs:
   a. The green LCD panel illuminates.
   b. The green **HDD** LED blinks momentarily, and processor speed and random-access memory information display momentarily at the LCD panel.
   c. After a few seconds, the LCD panel displays the following message pertaining to boot sequence selection (Figure 35):

Figure 35: LCD Panel During Boot Sequence

   d. Ignore the message. After ten seconds, the HAFM appliance performs the boot sequence from BIOS. During the boot sequence, the HAFM appliance performs additional POSTs and displays the following operational information at the LCD panel:
      — Host name.
      — System date and time.
      — LAN 1 and LAN 2 IP addresses.
      — Fan rotational speed.
      — CPU temperature.
      — Hard disk capacity.
      — Virtual and physical memory capacity.
4. After successful POST completion, the LCD panel displays a `Welcome!!` message, then continuously cycles through and displays HAFM appliance operational information.

Did POSTs detect a problem?

NO	YES
↓	An HAFM appliance hardware problem exists. Refer to the supporting documentation shipped with the HAFM appliance for instructions on resolving the problem. Exit MAP.

7

After rebooting the HAFM appliance at the LCD panel, log on to the HAFM appliance Windows 2000 desktop through a LAN connection to a browser-capable PC. Refer to the *HP StorageWorks Edge Switch 2/32 Installation Guide* for instructions on accessing the HAFM appliance desktop. HAFM starts and the HAFM Login dialog box displays.

Did the HAFM Login dialog box display?

YES	NO
↓	Go to step 9.

8

At the HAFM Login dialog box, type a user ID and password (obtained in "MAP 0000: Start MAP" on page 29, and both are case sensitive), and click **Login**. HAFM opens and the HAFM main window displays.

Did the main window display and does HAFM appear operational?

NO	YES
↓	The HAFM appliance appears operational. Exit MAP.

9

Perform one of the following:

- If the HAFM appliance has standalone diagnostic test programs resident on the hard drive, perform the diagnostics. Refer to supporting documentation shipped with the HAFM appliance for instructions.
- If the HAFM appliance does not have standalone diagnostic test programs resident on hard drive, go to step 10.

Did diagnostic test programs detect a problem?

NO	YES
↓	Refer to the supporting documentation shipped with the HAFM appliance for instructions to resolve the problem. Exit MAP.

10

Reboot the HAFM appliance.

1. At the Windows 2000 desktop, click **Start** at the left side of the task bar (bottom of the desktop), then click **Shut Down**. The Shut Down Windows dialog box displays.
2. Click the **Shut Down** option from the list box and click **OK**. The HAFM appliance powers down.
3. Wait approximately 30 seconds and press the power (⏻) button on the LCD panel to power on the HAFM appliance and perform POSTs. During POSTs:
   a. The green LCD panel illuminates.
   b. The green **HDD** LED blinks momentarily, and processor speed and random-access memory information display momentarily at the LCD panel.
   c. After a few seconds, the LCD panel displays the following message pertaining to boot sequence selection (Figure 36):

Figure 36: LCD Panel During Boot Sequence

   d. Ignore the message. After ten seconds, the HAFM appliance performs the boot sequence from BIOS. During the boot sequence, the HAFM appliance performs additional POSTs and displays the following operational information at the LCD panel:
      — Host name.
      — System date and time.
      — LAN 1 and LAN 2 IP addresses.
      — Fan rotational speed.
      — CPU temperature.
      — Hard disk capacity.
      — Virtual and physical memory capacity.
4. After successful POST completion, the LCD panel displays a `Welcome!!` message, then continuously cycles through and displays HAFM appliance operational information.

5. After rebooting the HAFM appliance at the LCD panel, log on to the HAFM appliance Windows 2000 desktop through a LAN connection to a browser-capable PC. Refer to the *HP StorageWorks Edge Switch 2/32 Installation Guide* for instructions on accessing the HAFM appliance desktop. HAFM starts and the HAFM Login dialog box displays.
6. At the HAFM Login dialog box, type a user ID and password (obtained in "MAP 0000: Start MAP" on page 29, and both are case sensitive), and click **Login**. HAFM opens and the HAFM main window displays.

Did the main window display and does HAFM appear operational?

NO **YES**

↓ The HAFM appliance appears operational. Exit MAP.

11

Re-install HAFM. Refer to "Install or Upgrade Software" on page 175 for instructions.

Did HAFM install and open successfully?

NO **YES**

↓ The HAFM appliance appears operational. Exit MAP.

12

Advise the customer and next level of support that the HAFM appliance hard drive should be restored to its original factory configuration. If the customer and support personnel do not concur, go to step 13.

1. Format the HAFM appliance hard drive. Refer to supporting documentation shipped with the HAFM appliance for instructions.
2. Restore the HAFM appliance hard drive using the *HAFM Appliance Restore/Boot CD* shipped with the HAFM appliance. Refer to the *readme.txt* file on the CD for instructions.
3. Install the *HAFM* application.

Did the HAFM appliance hard drive format, and did the operating system and HAFM install and open successfully?

NO **YES**

↓ The HAFM appliance appears operational. Exit MAP.

13

Additional analysis for the failure is not described in this MAP. Contact the next level of support. Exit MAP.

Repair Information

3

This chapter describes the repair and repair-related procedures for the HP StorageWorks Edge Switch 2/32, and associated field-replaceable units (FRUs). The following procedures are described:

Do not perform repairs until a failure is isolated to a FRU. If fault isolation was not performed, refer to “MAP 0000: Start MAP” on page 29.

Factory Defaults

Table 18 lists the defaults for the passwords, and IP, subnet, and gateway addresses.

Table 18: Factory-Set Defaults

Item	Default
Customer password	password
Maintenance password	level-2
IP address	10.1.1.10
Subnet mask	255.0.0.0
Gateway address	0.0.0.0

Procedural Notes

Note: HAFM and Element Manager screens in this manual may not match the screens on your server and workstation. The title bars have been removed and the fields may contain data that does not match the data seen on your system.

The following procedural notes are referenced in applicable repair procedures. The notes do not necessarily apply to all procedures in the chapter.

1. Before performing a repair procedure, read the procedure carefully and thoroughly to familiarize yourself with the information and reduce the possibility of problems or customer down time.
2. When performing procedures described in this chapter, heed all **WARNING** and **CAUTION** statements, and other statements listed in the preface of this manual.
3. After completing steps of a detailed procedure that is referenced from another procedure, return to the initial (referencing) procedure and continue to the next step of that procedure.

Using Log Information

The *HAFM*, *Element Manager*, and *EWS* applications provide access to logs that provide information for administration, operation, and maintenance personnel. Each log stores up to 1,000 entries. The most recent entry displays at the top of a log. If a log is full, a new entry overwrites the oldest entry.

Five logs are accessed through the *HAFM* application:

- **Audit Log**—Displays a history of user actions performed through the *HAFM* application. This information is useful for system administrators and users.
- **Event Log**—Displays events or error conditions recorded by the *HAFM Services* application. Entries reflect the status of the application and managed switches.

  Information associated with a call-home failure is intended for use by maintenance personnel to fault isolate the problem, while information provided in all other entries is generally intended for use by third-level support personnel to fault isolate more significant problems.
- **Session Log**—Displays session (login and logout) history for the HAFM appliance, including the date and time, username, and network address of each session. This information is useful for system administrators and users.
- **Product Status Log**—Displays an entry when the status of a switch changes. The log reflects the previous status and current status of the switch, and indicates the instance of an *Element Manager* application that should be opened to investigate a problem. The information is useful to maintenance personnel for fault isolation and repair verification.
- **Fabric Log**—Displays the time and nature of significant changes in the managed fabric.

For a description of the HAFM Logs and an explanation of the button functions at the bottom of the log window, refer to the *HP StorageWorks HA-Fabric Manager User Guide*.

Six logs are accessed through the *Element Manager* application:

- **Edge Switch 2/32 Audit Log**—Displays a history of all configuration changes made to a switch from the *Element Manager* application, a Simple Network Management Protocol (SNMP) management workstation open systems host, or the maintenance port. This information is useful for administrators and users.

- **Edge Switch 2/32 Event Log**—Displays a history of events for the switch, such as system events, degraded operation, FRU failures, FRU removals and replacements, port problems, Fibre Channel link incidents, and HAFM appliance-to-switch communication problems. All detected software and hardware failures are recorded in the Edge Switch 2/32 Event Log. The information is useful to maintenance personnel for fault isolation and repair verification.
- **Hardware Log**—Displays a history of FRU removals and replacements (insertions) for the switch. The information is useful to maintenance personnel for fault isolation and repair verification.
- **Link Incident Log**—Displays a history of Fibre Channel link incidents (with associated port numbers) for the switch. The information is useful to maintenance personnel for isolating port problems (particularly expansion port [E_Port] segmentation problems) and repair verification.
- **Threshold Alert Log**—Displays details of the threshold alert notifications. Besides the date and time that the alert occurred, the log also displays details about the alert as configured through the **Configure Threshold Alert(s)** option under the **Configure** menu.
- **Open Trunking Log**—Displays the average data rates of all traffic flows on ISLs (from a receive port to a target domain). Open Trunking also periodically adjusts routing tables to reroute data flows from congested links to lightly loaded links and optimize bandwidth use. The objective of Open Trunking is to make the most efficient possible use of redundant ISLs between neighboring switches, even if these ISLs have different bandwidths.

For a description of the Element Manager Logs and an explanation of the button functions at the bottom of the log window, refer to the *hp StorageWorks Edge Switch Element Manager User Guide*.

Three logs are accessed through the EWS interface:

- **EWS Event Log**—Displays events or errors recorded at the EWS interface. Entries reflect the status of the interface and managed switch. The log stores up to 200 entries, and the most recent entry appears at the top of the log.
- **EWS Open Trunking Re-Route Log**—Displays interswitch link (ISL) congestion events that cause Fibre Channel traffic to be routed through an alternate ISL. Entries reflect the traffic re-route status at the managed switch.
- **EWS Link Incident Log**—Displays Fibre Channel link incident events recorded at the EWS interface. Entries reflect the cause of the link incident.

For a description of the EWS Logs and an explanation of the button functions at the bottom of the log window, refer to the *hp StorageWorks Embedded Web Server User Guide*.

Viewing Logs

You can view log data through the Master Log on the main window. However, if you want to see only certain types of events, for example only login/logout events (session events), open a specific log through the View Logs dialog box.

To view a log, perform the following:

1. Choose **Monitor > Logs**, then choose one of the options. The View Logs dialog box displays, as shown in Figure 37.

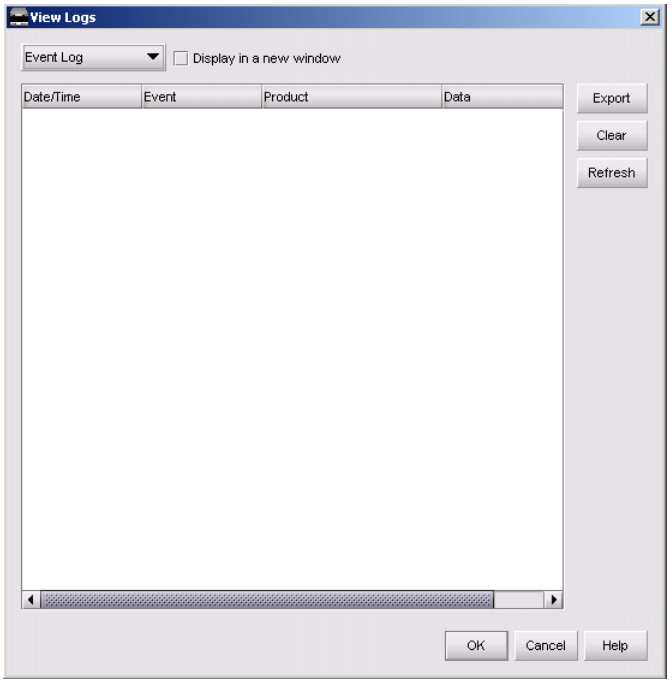


Figure 37: View Logs dialog box

- To view a different log, choose a log from the drop-down list.
- To view multiple logs simultaneously, choose the **Display in a new window** check box and choose another log from the drop-down list.
- To clear the log, click **Clear**.

- To refresh the log, click **Refresh**.
- To export log entries, refer to "Exporting Log Data" on page 134.

2. Click **OK** to close the dialog box.

Exporting Log Data

You can export HAFM log data in tab-delimited format. This feature is useful for providing the data to a third-party or including it in a report.

1. Choose **Monitor > Logs**, then choose one of the options. The View Logs dialog box displays, as shown in Figure 37.
2. Click **Export**. The Save dialog box displays.
3. Browse to the folder where you want to save the file. Type a file name in the **File Name** field.
4. Click **Save**. The file is exported in tab-delimited format. To view it in table format, open the file in Microsoft Excel.

Obtaining Port Diagnostic Information

Fibre channel port diagnostics are performed at the switch and *Element Manager* application. These diagnostics include:

- Inspecting port LEDs at the switch front panel or emulated port LEDs at the HAFM **Hardware View**.
- Inspecting parameters at the HAFM appliance (Edge Switch 2/32 *Element Manager* application).
- Inspecting parameters at the EWS interface (refer to the *HP StorageWorks Embedded Web Server User Guide* for more information).
- Performing channel wrap tests. The tests apply only to a switch configured for FICON management style.

Port LEDs

To obtain port operational information, inspect port LEDs at the switch front panel or emulated port LEDs at the HAFM **Hardware View**.

Amber and green LEDs adjacent to each port indicate operational status as follows:

- The green LED illuminates (or blinks if there is active traffic) and the amber LED extinguishes to indicate normal port operation.
- The amber LED illuminates and the green LED extinguishes to indicate a port failure.
- Both LEDs extinguish to indicate a port is operational but not communicating (no SFP installed, no cable attached, loss of light, port blocked, or link recovery in process).
- The amber LED flashes and the green LED illuminates (or blinks if there is active traffic) to indicate beaconing is set for the port.

The amber LED flashes and the green LED extinguishes to indicate a port is running online diagnostics, or beaconing is set and the port is not communicating (no SFP installed, no cable attached, loss of light, port blocked, or link recovery in process).

Obtaining Port Information

To obtain port operational information at the HAFM appliance (Edge Switch 2/32 *Element Manager* application), inspect parameters at the:

- **Port List View**
- **Performance View**
- Port Properties dialog box
- Port Technology dialog box

Viewing the Port List View

The **Port List View** provides status information for all switch ports. The information is useful to maintenance personnel for isolating port problems.

To open the **Port List View**, perform the following:

1. At the **Hardware View**, click the **Port List** tab. The **Port List View** displays, as shown in Figure 38.

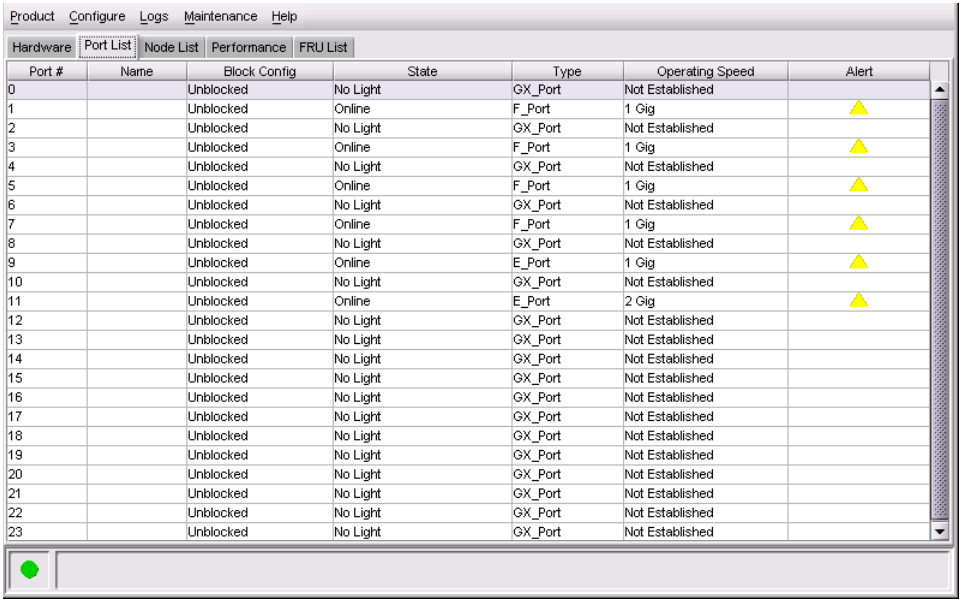


Figure 38: Port List View

The **Port List View** provides status information in the following columns:

- **#**—The switch port number (**0** through **139** inclusive).
- **Addr**—The switch logical port address in hexadecimal format (FICON management style only).
- **Name**—The port name configured through the Configure Ports dialog box.
- **Block Config**—The port status (Blocked or Unblocked).
- **State**—The operating state of the port. Valid states are:
  - Online, Offline, or Testing
  - Beaconing
  - Invalid Attachment
  - Link Incident or Link Reset
  - No Light, Not Operational, or Port Failure
  - Segmented E_Port
- **Type**—The type of port. Valid port types are a generic port (G_Port) not connected to a Fibre Channel device, director, or switch (therefore light is not transmitted); a fabric port (F_Port) connected to a device; or an expansion port (E_Port) connected to a director or switch to form an interswitch link (ISL).
- **Operating Speed**—The operating speed of the port (Not Established, 1, or 2 Gb/sec.).
- **Alert—**If Link Incident (LIN) alerts are configured for the port through the Configure Ports dialog box, a yellow triangle displays in the column when a link incident occurs. A yellow triangle also displays if beaconing is enabled for the port. A red and yellow diamond displays if the port fails.

Double-click anywhere in a row for an installed port to open the Port Properties dialog box.

Right-click anywhere in a row for an installed port to open a menu to:

- Open the Port Properties, Node Properties, or Port Technology dialog boxes.
- Block or unblock the port.
- Enable or disable port beaconing.
- Perform port diagnostics.
- Enable or disable port channel wrapping. This menu option displays only when the switch is configured for FICON management style.

- Swap one Fibre Channel port address with another. This menu option displays only when the switch is configured for FICON management style.
- Clear link incident alerts.
- Reset the port.
- Configure port binding.
- Clear threshold alerts.

Viewing the Performance View

To view performance data, perform the following:

1. At the **Hardware View**, click the **Performance** tab. The **Performance View** displays, as shown in Figure 39.

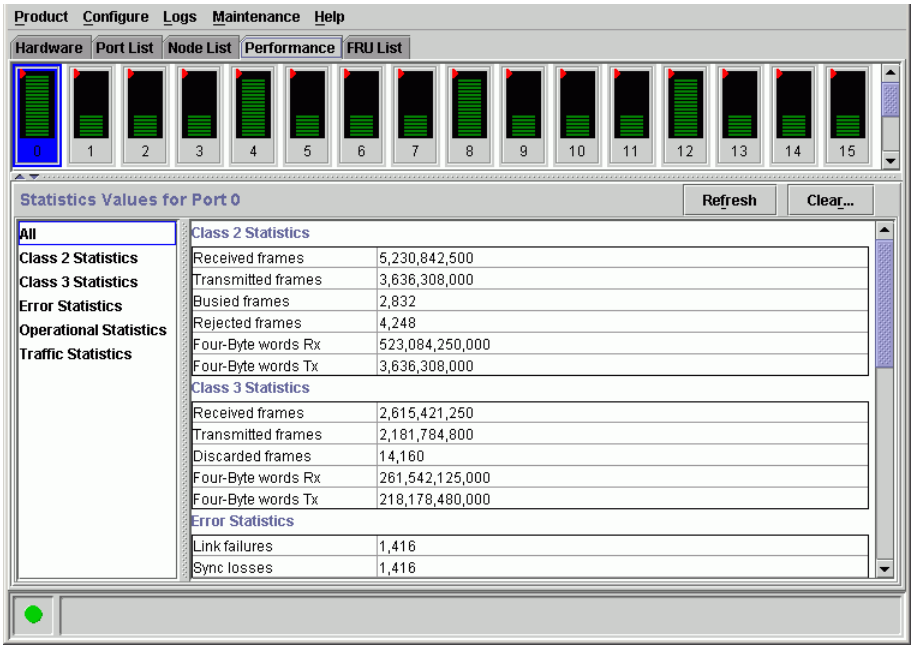


Figure 39: Performance View

Each port bar graph in the upper portion of the view displays the instantaneous transmit or receive activity level for the port, and is updated every five seconds. The relative value displayed is the greater of either the transmit or receive activity (whichever value is greatest when sampled).

Each port graph has 20 green-bar level indicators corresponding to 5% of the maximum throughput for the port (either transmit or receive). If any activity is detected for a port, at least one green bar appears. A red indicator on each port bar graph (high-water mark) remains at the highest level the graph has reached since the port was set online. The indicator does not display if the port is offline, and is reset to the bottom of the graph if the port detects a loss of light.

When the mouse cursor is passed over a port bar graph (flyover), the graph highlights with a blue border and an information pop-up displays the port operational state or WWN of the attached device. Click a port bar graph to display statistics values for the port. Right-click a port bar graph to open a pop-up menu to:

- Open the Port Properties, Node Properties, or Port Technology dialog boxes.
- Block or unblock the port.
- Enable or disable port beaconing.
- Perform port diagnostics.
- Enable or disable port channel wrapping (when the switch is configured for FICON management style).
- Swap one Fibre Channel port address with another (when the switch is configured for FICON management style).
- Clear link incident alerts.
- Reset the port.
- Enable or disable port binding.
- Clear threshold alerts.

The page displays the following tables of cumulative port statistics and error count values for a selected port:

- **Class 2 statistics**—These entries provide information about Class 2 traffic, including:
  - — Class 2 frames received and transmitted.
  - — Four-byte words received and transmitted.
  - — Busied and rejected frames.
- **Class 3 statistics**—These entries provide information about Class 3 traffic, including:
  - — Class 3 frames received and transmitted.
  - — Four-byte words received and transmitted.

- Discarded frames.

- **Error statistics**—The **Performance View** displays the following error statistics for the port:
  - **Link failures**—Link failures are recorded in response to an NOS, protocol time-out, or port failure. At the **Hardware View**, a yellow triangle appears to indicate a link incident, or a blinking red and yellow diamond displays to indicate a port failure.
  - **Sync losses**—Synchronization losses are detected because an attached device was reset or disconnected from the port. At the **Hardware View**, a yellow triangle displays to indicate a link incident.
  - **Signal losses**—Signal losses are detected because an attached device was reset or disconnected from the port. At the **Hardware View**, a yellow triangle displays to indicate a link incident.
  - **Primitive sequence errors**—Incorrect primitive sequences are received from an attached device, indicating Fibre Channel link-level protocol violations. At the **Hardware View**, a yellow triangle displays to indicate a link incident.
  - **Discarded frames**—Received frames could not be routed and were discarded because the frame timed out (insufficient buffer-to-buffer credit) or the destination device was not logged into the switch.
  - **Invalid transmission words**—Several transmission words were received with encoding errors, indicating an attached device is not operating in conformance with the Fibre Channel specification.
  - **CRC errors**—Received frames failed CRC validation, indicating the frames arrived at the switch port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber-optic cable, or a poor cable connection.
  - **Delimiter errors**—Received frames had frame delimiter errors, indicating the frame arrived at the switch port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber-optic cable, or a poor cable connection.
  - **Address ID errors**—Received frames had unavailable or invalid Fibre Channel destination addresses, or invalid Fibre Channel source addresses. This typically indicates the destination device is unavailable.

- — **Frames too short**—Received frames were less than the Fibre Channel minimum size, indicating the frame arrived at the switch port corrupted. Frame corruption may be caused by device disconnection, an optical transceiver failure at the device, a bad fiber-optic cable, or a poor cable connection.

- **Operational statistics**—These entries provide information about port operation, including:
  - — Offline sequences received and transmitted.
  - — Link resets received and transmitted.
  - — LIPs generated and detected.
- **Traffic statistics**—These entries provide information about port traffic, including:
  - — Percent link utilization (receive and transmit).
  - — Fibre Channel frames received and transmitted.
  - — Four-byte words received and transmitted.
  - — Flows rerouted to and from ISLs.

Viewing Port Properties

To open the Port Properties dialog box, perform the following:

1. Double-click a port graphic at the **Hardware View** or a port row at the **Port List View**. The Port Properties dialog box displays, as shown in Figure 40.

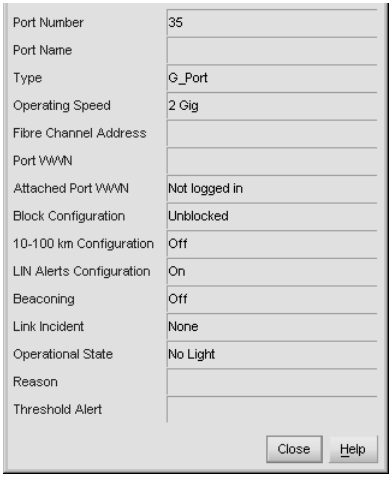


Figure 40: Port Properties dialog box

The Port Properties dialog box provides the following information:

Note: If the Open Trunking feature is installed, an additional item, **Congested Threshold %**, displays in the Port Properties dialog box.

- **Port Number**—The switch port number (**0**-**31** inclusive).
- **Port Name**—The user-defined name or **description** for the port.
- **Type**—The Port type (**G_Port**, **F_Port**, or **E_Port**) type of port (G_Port if nothing is attached to the port, F_Port if a device is attached to the port, and E_Port if the port is connected to another director or switch as part of an ISL).
- **Operating Speed**—The operating speed of the port (**Not Established**, **1 Gb/s**, or **2 Gb/s**.).
- **Port WWN**—The Fibre Channel WWN for the switch port.
- **Block Configuration**—A user-configured state for the port (**Blocked** or **Unblocked**).
- **LIN Alerts Configuration**—A user-specified state for the port (**On** or **Off**), configured through the Configure Ports dialog box.
- **FAN Configuration**—A user-configured state for FAN configuration (**Enabled** or **Disabled**).

- **Beaconing**—User-specified for the port (**On** or **Off**). When beaconing is enabled, a yellow triangle appears adjacent to the status field.
- **Link Incident**—If no link incidents are recorded, **None** appears in the status field. If a link incident is recorded, a summary appears describing the incident, and a yellow triangle appears adjacent to the status field. Valid summaries are:
  - Implicit incident.
  - Bit-error threshold exceeded.
  - Link failure–loss of signal or loss of synchronization.
  - Link failure–not-operational primitive sequence received.
  - Link failure–primitive sequence time-out.
  - Link failure–invalid primitive sequence received for the current link state.
- **Operational State**—The state of the port (**Online**, **Offline**, **Beaconing**, **Invalid Attachment**, **Link Incident**, **Link Reset**, **No Light**, **Not Operational**, **Port Failure**, **Segmented E_Port, or Testing**). A yellow triangle appears adjacent to the status field if the port is in a non-standard state that requires attention. A red and yellow diamond appears adjacent to the status field if the port fails.
- **Reason**—A summary appears describing the reason if the port state is **Segmented E_Port**, **Invalid Attachment**, or **Inactive**. For any other port state, the reason field is blank or N/A. Invalid Attachment Messages are explained in Table 19.

Table 19: Invalid Attachment Messages and Explanations

Message	Explanation
01 Unknown.	Invalid attachment reason cannot be determined.
02 ISL connection not allowed on this port.	Port is configured as an F_Port, but connected to switch or director.
03 ELP rejected by the attached switch.	This director or switch transmitted an exchange link protocol (ELP) frame that was rejected by the switch at the other end of the ISL (Invalid Attachment only).
04 Incompatible switch at the other end of the ISL.	Interop mode for this switch is set to Open Fabric mode and the switch at the other end of the ISL is a switch configured for Homogeneous Fabric mode.

Table 19: Invalid Attachment Messages and Explanations (Continued)

Message	Explanation
05 External loopback adapter connected to the port.	A loopback plug is connected to the port and there is no diagnostic test running.
06 N_Port connection not allowed on this port.	The port type configuration does not match the actual port use. Port is configured as an E_Port, but attaches to a node device.
07 Non-homoge-neous switch at other end of the ISL.	The cable is connected to a non-homogeneous switch and interop mode is set to homogeneous fabric mode.
08 ISL connection not allowed on this port.	This port type configuration does not match the actual port use (the port is configured as an F_Port, but attaches to a switch or director).
10 Port binding viola-tion–unauthorized WWN.	The WWN entered to configure port binding is not valid or a nickname was used that is not configured through the Element Manager for the attached device.
11 Unresponsive node connected to port.	Possible causes are: ■ Hardware problem on switch or on a connected node where ELP frames are not delivered, the response is not received, or a fabric login (FLOGI) cannot be received. There may be problems in switch SBAR. ■ Faulty or dirty cable connection. ■ Faulty host bus adapters that do not send out FLOGI within reasonable time frame.

- **Threshold Alert**—If a threshold alert exists for the port, an alert indicator (yellow triangle) and the configured name for the alert appear.

Viewing the Port Technology

To open the Port Technology dialog box, perform the following:

1. Right-click a port graphic at the **Hardware View** or a port row at the **Port List View**. A menu displays,
2. Choose **Port Technology**. The Port Technology dialog box displays, as shown in Figure 41.

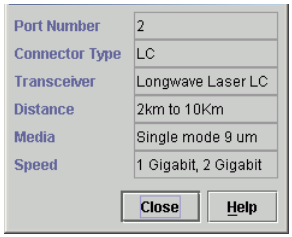


Figure 41: Port Technology dialog box

The Port Technology dialog box provides the following information:

- **Port Number**—The switch port number (**0**-**31** inclusive).
- **Connector type**—Type of port connector (**LC**, **Unknown**, or **Internal Port**).
- **Transceiver**—Type of port transceiver (**Shortwave Laser**, **Longwave Laser**, Long Distance Laser, Unknown, or None).
- **Distance**—Port transmission distance (Short, Intermediate, Long, Very Long, or **Unknown**).
- **Media**—Type of optical cable used (**Singlemode**, **multimode 50-micron**, **multimode 62.5-micron**, or **Unknown**).
- **Speed**—Operating speed (**Not Established**, **1 Gb/s**, or **2 Gb/s**).

Perform Loopback Tests

This section describes procedures to perform an:

- **Internal loopback test**–An internal loopback test checks internal port, serializer, and deserializer circuitry and checks for the presence of an optical transceiver, but does not check fiber-optic components of the installed transceiver. Operation of the attached device is disrupted during the test.
- **External loopback test–**An external loopback test checks all port circuitry, including fiber-optic components of the installed optical transceiver. To perform the test, the attached device must be quiesced and disconnected from the port, and a singlemode or multimode loopback plug must be inserted in the port.

Internal Loopback Test

To perform an internal loopback test for a single port:

1. Notify the customer that a disruptive internal loopback test is to be performed on a port. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port and sets the attached devices offline.

Note: An SFP transceiver must be installed in the port during the test. A switch can remain attached during the test.

---

2. Open the *HAFM* application. The View All - HAFM 8 main window displays.
3. At the HAFM physical map, right-click the product icon representing the switch to be tested, then click **Element Manager** from the pop-up menu. The application opens.
4. Click **Maintenance > Port Diagnostics**. The **Port Diagnostics** dialog box displays.
5. Type the port number to be tested, or select all ports at the **Port Select** area of the dialog box

6. At the **Diagnostics Test** list box, select **Internal Loopback**.
7. Click **Next**. The message `Press START TEST to begin diagnostics` displays, and the **Next** button changes to a **Start Test** button.
8. Click **Start Test**. The test begins and:
   - The **Start Test** button changes to a **Stop Test** button.
   - The message `Port xx: TEST RUNNING` displays.
   - A red progress bar (indicating percent completion) travels from left to right across the **Completion Status** field.

Note: Click **Stop Test** at any time to abort the loopback test.

9. When the test completes, results appear as `Port xx: Passed!` or `Port xx: Failed!` in the message area of the dialog box.
10. When finished, click **Cancel** to close the **Port Diagnostics** dialog box and return to the **Hardware View**.
11. Reset the port:
    a. At the **Hardware View**, right-click the port graphic. A pop-up menu displays.
    b. Click the **Reset Port** option. A message box displays, indicating a link reset operation will occur.
    c. Click **OK**. The port resets.
12. Notify the customer the test is complete and the attached device can be set online.

External Loopback Test

To perform an external loopback test for a single port:

1. Notify the customer that a disruptive external loopback test will be performed on a port and the fiber-optic cable or cables will be disconnected. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port and sets attached devices offline.

Note: At the start of the loopback test, the port can be online, offline, blocked, or unblocked.

2. Open the *HAFM* application. The View All - HAFM 8 main window displays.
3. At the HAFM physical map, right-click the product icon representing the switch to be tested, then click **Element Manager** from the pop-up menu. The application opens.
4. Disconnect the fiber-optic jumper cable from the port.
5. Depending on the port technology, insert a singlemode or multimode loopback plug into the port receptacle.
6. Click **Maintenance > Port Diagnostics**. The **Port Diagnostics** dialog box displays.
7. Type the port number to be tested or select all ports at the **Port Select** area of the dialog box.
8. At the **Diagnostics Test** list box, select the **External Loopback** option.
9. Click **Next**. At the **Port Diagnostics** dialog box, the message `Loopback plug(s) must be installed on ports being diagnosed` displays.
10. Verify a loopback plug is installed and click **Next**. The message `Press START TEST to begin diagnostics` displays, and the **Next** button changes to a **Start Test** button.
11. Click **Start Test**. The test begins and:
    - The **Start Test** button changes to a **Stop Test** button.
    - The message `Port xx: TEST RUNNING` displays.
    - A red progress bar (indicating percent completion) travels from left to right across the **Completion Status** field.

Note: Click **Stop Test** at any time to abort the loopback test.

12. When the test completes, results appear as `Port xx: Passed!` or `Port xx: Failed!` in the message area of the dialog box.
13. When finished, click **Cancel** to close the **Port Diagnostics** dialog box.

14. Remove the loopback plug and reconnect the fiber-optic jumper cable from the device to the port.
15. Reset the port:
    a. At the **Hardware View**, right-click the port graphic. A pop-up menu displays.
    b. Click the **Reset Port** option. A message box displays, indicating a link reset operation will occur.
    c. Click **OK**. The port resets.
16. Notify the customer the test is complete and the device can be reconnected to the switch and set online.

Swapping Ports (FICON)

Use the port swap procedure to swap a device connection and logical port address from a failed Fibre Channel port to an operational port. Because both ports are blocked during the procedure, edge switch communication with the attached device is momentarily disrupted.

To perform the port swap procedure for a pair of edge switch ports:

1. Notify the customer a port swap procedure will be performed and a fiber optic cable or cables will be disconnected. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the ports and sets attached devices offline.
2. Open the *HAFM* application. The View All - HAFM 8 main window displays.
3. Double-click the icon representing the switch for which the loopback test will be performed. The **Hardware View** for the selected switch displays.
4. Click **Maintenance** and choose **Swap Ports**. The Swap Ports dialog box displays.
5. Enter the logical port addresses (in hexadecimal format) of the pair of ports to be swapped at the **First address** and **Second address** fields. The ports are automatically blocked during the procedure.
6. Choose the **Unblock after swap** check boxes to unblock the ports when the procedure completes.
7. Click **Next**. At the Swap Ports dialog box, the message `Continuing this procedure requires varying the selected ports offline. Ask the system operator to vary the link(s) offline, then press Next.` displays.

8. Click **Next**. At the Swap Ports dialog box, the message `Move the port cable(s). Then press Next.` displays.
9. Swap the fiber optic cables between the selected ports, then click **Next**.

At the Swap Ports dialog box, the message `Ports swapped successfully.` displays. Click **Next** to close the window and return to the **Hardware View**.

Collecting Maintenance Data

When the switch operational firmware detects a critical error or FRU failure, the switch automatically copies the contents of dynamic random access memory (DRAM) to a dump area in FLASH memory on the active CTP card, then initiates a failover to the operational FRU. The switch then transfers (through the Ethernet connection) the captured dump file from FLASH memory to the HAFM appliance hard drive.

Note: An optional full-volatility feature is often required at military sites that process classified data. If the feature is enabled through a product feature enablement (PFE) key, a memory dump file (that possibly includes classified Fibre Channel frames) is not included as part of the data collection procedure.

Perform the maintenance data collection procedure after a firmware fault is corrected or a failed FRU is replaced to capture the data for analysis by third-level support personnel. Maintenance data includes the dump file, Hardware Log, Audit Log, and an engineering log viewable only by support personnel. To collect maintenance data:

1. Open the *HAFM* application. The View All - HAFM 8 main window displays.
2. Double-click the icon representing the switch for which the data collection procedure will be performed. The **Hardware View** for the selected switch displays.
3. Choose **Maintenance > Data Collection**. The Save Data Collection dialog box displays, as shown in Figure 42.

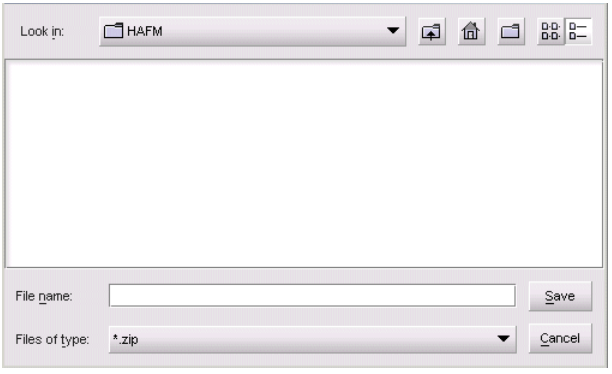


Figure 42: Save Data Collection dialog box

4. Remove the backup disk from the HAFM appliance backup drive and insert a blank backup disk.
5. At the Save Data Collection dialog box, select the backup drive from the **Look in:** drop-down menu, then type a descriptive name for the collected maintenance data in the **File name** field. Ensure the file name has a *.zip* extension, then click **Save**.
6. A dialog box displays, as shown in Figure 43, with a progress bar that shows percent completion of the data collection process. When the process reaches 100%, **Cancel** changes to **Close**.

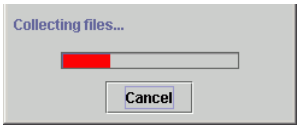


Figure 43: Data Collection dialog box

7. Click **Close** to close the dialog box.
8. Remove the backup disk with the newly collected maintenance data from the HAFM appliance backup drive. Return the backup disk with the failed FRU to HP for failure analysis.

To ensure the backup application operates normally, replace the original backup disk in the HAFM appliance backup drive.

Clean Fiber-Optic Components

Perform this procedure as directed in this publication and when connecting or disconnecting fiber-optic cables from port optical transceivers (if necessary). To clean fiber-optic components:

1. Obtain the appropriate tools (portable can of oil-free compressed air and alcohol pads) from the fiber-optic cleaning kit.
2. Disconnect the fiber-optic cable from the transceiver. Use compressed air to blow any contaminants from the connector as shown in ❶ on Figure 44.
   a. Keep the air nozzle approximately 50 millimeters (two inches) from the end of the connector and hold the can upright.
   b. Blow compressed air on the surfaces and end of the connector continuously for approximately five seconds.

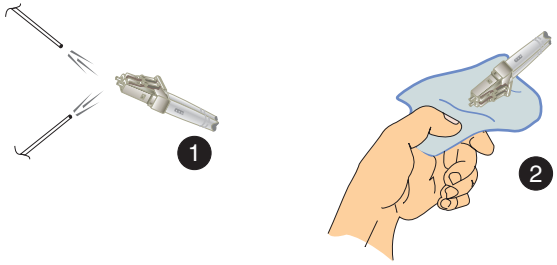


Figure 44: Clean fiber-optic components

3. Gently wipe the end-face and other surfaces of the connector with an alcohol pad as shown in ❷ on Figure 44. Ensure the pad makes full contact with the surface to be cleaned. Wait approximately five seconds for surfaces to dry.
4. Repeat step 2 and step 3 of this procedure (second cleaning).
5. Repeat step 2 and step 3 of this procedure again (third cleaning), then reconnect the fiber-optic cable to the port.

Power-On Procedure

To power-on the switch:

1. One alternating current (AC) power cord is required for each power supply. Ensure power cord(s) are available to connect the switch to facility power.

WARNING: A Hewlett-Packard-supplied power cord is provided for each switch power supply. To prevent electric shock when connecting the switch to primary facility power, use only the supplied power cord(s), and ensure the facility power receptacle is the correct type, supplies the required voltage, and is properly grounded.

Note: Turn on both power switches at the rear of the unit. The unit powers on and performs power-on self-tests (POSTs). If two power cords are used for high availability, plug the cords into separate facility power circuits.

2. During POSTs:
   - The green power (**PWR**) LED on the switch front panel illuminates.
   - The amber system error (**ERR**) LED on the switch front panel blinks momentarily while the switch is tested.
   - The green LEDs associated with the Ethernet port blink momentarily while the port is tested.
   - The green and amber LEDs associated with the ports blink momentarily while the ports are tested.
1. After successful POST completion, the green power (**PWR**) LED remains illuminated and all amber LEDs extinguish.
2. If a POST error or other malfunction occurs, go to "MAP 0000: Start MAP" on page 29 to isolate the problem.

Note: When powering on the switch after removing and replacing a faulty FRU, the amber system error LED may remain illuminated. Clear the system error LED as part of the replacement procedure.

Power-Off Procedure

To power-off the switch:

1. Notify the customer the switch is to be powered off. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the switch and sets attached devices offline.
2. Set the switch offline ("Set Offline State" on page 160).
3. Turn off both power switches at the rear of the unit. If servicing the switch, disconnect the power cord(s) from the input power module at the rear of the switch. This step is not required when performing a power cycle.

IML, IPL, or Reset the Switch

This section describes procedures to IML, IPL, or reset the Edge Switch. An IML or reset is performed at the switch front panel using the **IML/RESET** button. An IPL is performed from the HAFM appliance (*Element Manager* application). The EWS interface does not provide an IML, IPL, or switch reset function.

Caution: A reset should only be performed if a CTP card failure is indicated. Do not reset the switch unless directed to do so by a procedural step or the next level of support.

An IML and IPL are functionally equivalent. The operations do not cause power-on diagnostics to execute and are not disruptive to Fibre Channel traffic.

Both the IML and IPL operations:

- Reload switch firmware from FLASH memory.
- Reset the Ethernet LAN interface, causing the connection to the HAFM appliance to drop momentarily until the connection automatically recovers.

A switch reset is more disruptive and resets the:

- Microprocessor and functional logic for the CTP card. It also reloads the firmware from FLASH memory.
- Ethernet LAN interface, causing the connection to the HAFM appliance to drop momentarily until the connection automatically recovers.
- Ports, causing all Fibre Channel connections to drop momentarily until the connections automatically recover. This causes attached devices to log out and log back in. After the login, data frames lost during switch reset must be retransmitted.

Switch IML

To IML the switch from the front panel:

1. Press and hold the **IML/RESET** button until the amber **ERR** LED blinks at twice the unit beaconing rate (approximately three seconds).
2. Release the button to IML the switch. During the IML, the switch-to-HAFM appliance Ethernet link drops momentarily and the following occur at the **Hardware View**:
   - — As the network connection drops, the **status** table turns yellow, the **Status** field displays `No Link`, and the **State** field displays `Link Timeout`.
   - — The status bar at the bottom of the window displays a grey square, indicating that the switch status is unknown.
   - — Illustrated FRUs disappear, and appear again, as the connection is re-established.

Switch IPL

To IPL the switch from the HAFM appliance (Edge Switch 2/32 *Element Manager* application):

3. Open the *HAFM* application. The View All - HAFM 8 main window displays.
4. Double-click the icon representing the switch requiring an IPL. The **Hardware View** for the selected switch displays.
5. Choose **Maintenance > IPL**. The Information dialog box displays.
6. Click **Yes** to IPL the switch. During the IPL, the switch-to-HAFM appliance Ethernet link drops momentarily and the following occur at the **Hardware View**:
   - — As the network connection drops, the **status** table turns yellow, the **Status** field displays `No Link`, and the **State** field displays `Link Timeout`.
   - — The status bar at the bottom of the window displays a grey square, indicating switch status is unknown.
   - — Illustrated FRUs disappear, and appear again as the connection is re-established.

Switch Reset

To reset the switch from the front panel:

1. Press and hold the **IML/RESET** button for approximately ten seconds.
   - — After holding the button for three seconds, the amber **ERR** LED blinks at twice the unit beaconing rate.
   - — After holding the button for ten seconds, the **ERR** LED stops blinking, and all front panel LEDs illuminate.
2. Release the button to reset the switch. During the reset:
   - — The green power (**PWR**) LED on the switch front panel illuminates.
   - — The amber system error (**ERR**) LED on the switch front panel blinks momentarily while the switch is tested.
   - — The green LEDs associated with the Ethernet port blink momentarily while the port is tested.
   - — The green and amber LEDs associated with the ports blink momentarily while the ports are tested.
   - — The switch-to-HAFM appliance Ethernet link drops momentarily and the following occur at the **Hardware View**:
     - — As the network connection drops, the **status** table turns yellow, the **Status** field displays `No Link`, and the **State** field displays `Link Timeout`.
     - — The status bar at the bottom of the window displays a grey square, indicating switch status is unknown.
     - — Illustrated FRUs disappear, and appear again as the connection is re-established.

Set the Switch Online or Offline

This section describes procedures to set the switch online or offline. These operating states are described as follows:

- **Online–**when the switch is set online, an attached device can log in to the switch if the port is not blocked. Attached devices can communicate with each other if they are configured in the same zone.
- **Offline–**when the switch is set offline, all switch ports are set offline. The switch transmits the offline sequence (OLS) to attached devices, and the devices cannot log in to the switch.

Note: When the switch is set offline, the operation of attached Fibre Channel devices is disrupted. Do not set the switch offline unless directed to do so by a procedural step or the next level of support.

Set Online State

To set the switch online:

1. Open the *HAFM* application. The View All - HAFM 8 main window displays.
2. Double-click the icon representing the switch to be set online. The **Hardware View** for the selected switch displays.
3. Choose **Maintenance > Set Online State**. If the switch is offline, the Set Online State dialog box displays, as shown in Figure 45, indicating the state is **OFFLINE**.

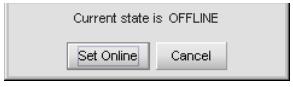


Figure 45: Set Online State dialog box (offline)

4. Click **Set Online**. A Warning dialog box displays, indicating the switch will be set online.
5. Click **OK**. As the switch comes online, observe the *Element Manager* application. The **State** field of the **Edge Switch 2/32 Status** table displays **ONLINE**.

Set Offline State

To set the switch offline:

1. Notify the customer the switch is to be set offline. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the switch and sets attached devices offline.
2. Open the *HAFM* application. The View All - HAFM 8 main window displays.
3. Double-click the icon representing the switch to be set offline. The **Hardware View** for the selected switch displays.
4. Choose **Maintenance > Set Online State**. If the switch is online, the **Set Online State** dialog box displays, indicating the state is **ONLINE**.

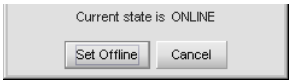


Figure 46: Set Offline Warning dialog box

5. Click **Set Offline**. A **Warning** dialog box displays, indicating the switch is to be set offline.
6. Click **OK**. As the switch goes offline, inspect the *Element Manager* application. The **State** field of the **Status** table displays **OFFLINE**.

Block and Unblock Ports

This section describes procedures to block or unblock the switch Fibre Channel ports. Blocking a port prevents the attached device or fabric switch from communicating. A blocked port continuously transmits the offline sequence (OLS).

Note: When a port is blocked, the operation of an attached Fibre Channel device is disrupted. Do not block a port unless directed to do so by a procedural step or the next level of support.

Block a Port

To block a port:

1. Notify the customer the port is to be blocked. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the port and sets the attached device offline.
2. Open the *HAFM* application. The View All - HAFM 8 main window displays.
3. Double-click the icon representing the switch for which a port will be blocked. The **Hardware View** for the selected switch displays.
4. Move the pointer over the port and right-click the mouse to open a list of menus.
5. Select **Block Port**. The Block Port warning box displays.
6. Click **OK**. The following occur to indicate the port is blocked (and offline):
   - The emulated green LED associated with the port extinguishes at the **Hardware View**.
   - The green LED associated with the port extinguishes at the switch.
   - A check mark displays in the check box adjacent to the **Block Port** menu option.

Unblock a Port

To unblock a port:

7. Open the *HAFM* application. The View All - HAFM 8 main window displays.
8. Double-click the icon representing the switch for which a port will be unblocked. The **Hardware View** for the selected switch displays.
9. Move the pointer over the port and right-click the mouse to open a list of menu options.
10. Click **Block Port**. Note the check mark in the box adjacent to the menu item, indicating the port is blocked. The Unblocking Port warning box displays.
11. Click **OK**. The following occur to indicate the port is unblocked (and online):
    - The emulated green LED associated with the port illuminates at the **Hardware View**.
    - The green LED associated with the port illuminates at the switch.
    - The check box adjacent to the **Block Port** menu option becomes blank.

Manage Firmware Versions

Firmware is the internal operating code stored in FLASH memory on the switch's CTP card. Up to eight versions can be stored on the HAFM appliance hard drive and made available for download to a switch through the switch *Element Manager* application. Service personnel can perform the following firmware management tasks:

- Determine the firmware version active on a switch.
- Add to and maintain a library of up to eight firmware versions on the HAFM appliance hard drive.
- Download a firmware version to a selected switch.

Note: The HP StorageWorks HAFM, director, and edge switch release notes include the latest information about supported firmware and HAFM versions.

Determine a Switch Firmware Version

To determine a switch firmware version:

1. Open the *HAFM* application. The View All - HAFM 8 main window displays.
2. Double-click the icon representing the switch to be inspected for firmware version. The **Hardware View** for the selected switch displays.
3. Choose **Maintenance > Firmware Library**. The **Firmware Library** dialog box displays, as shown in Figure 47.

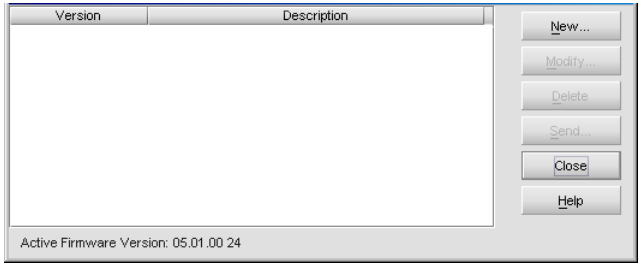


Figure 47: Firmware Library dialog box

4. The firmware version displays at the lower left corner of the dialog box in XX.YY.ZZ format, where XX is the version level, YY is the release level, and ZZ is the patch level.

5. Click **Close** to return to the **Hardware View**.

Add a Firmware Version

The firmware version shipped with the switch is provided on the Edge Switch 2/32 documentation kit CD. Subsequent firmware versions for upgrading the switch are provided to customers through the HP web site.

Note: When adding a firmware version, follow all the instructions in the release notes that accompany the firmware version. This information supplements information in this general procedure.

To add a switch firmware version to the library stored on the HAFM appliance hard drive:

1. Obtain the new firmware version from the HP web site:

Note: The following path is subject to change.

---

   a. At the HAFM appliance or other personal computer (PC) with Internet access, open the HP web site. The uniform resource locator (URL) is:

      http://h18006.www1.hp.com/storage/saninfrastructure.html

---

Note: If required, obtain the customer-specific member name and password from the customer or next level of support.

---

   b. Follow links to the Edge Switch 2/32 firmware.

   c. Click the Edge Switch 2/32 Firmware Version XX.YY.ZZ entry, where XX.YY.ZZ is the desired version. The **Windows Save As** dialog box displays.

   d. Ensure the correct directory path is specified at the **Save** in field and the correct file is specified in the **File name** field. Click **Save**. The new firmware version is downloaded and saved to the HAFM appliance or PC hard drive.

e. If the new firmware version was downloaded to a PC (not the HAFM appliance), transfer the firmware version file to the HAFM appliance by CD-ROM or other electronic means.

2. Open the *HAFM* application. The View All - HAFM 8 main window displays.
3. Double-click the icon representing the switch to which the firmware version will be added. The **Hardware View** for the selected switch displays.
4. Choose **Maintenance > Firmware Library**. The **Firmware Library** dialog box displays (Figure 47).
5. Click **New**. The **New Firmware Version** dialog box displays.

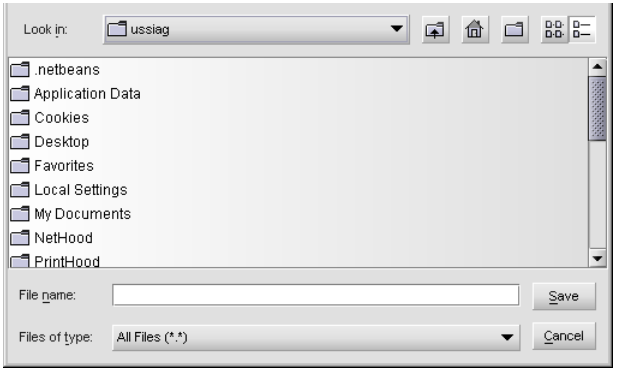


Figure 48: New Firmware Version dialog box

6. Select the desired firmware version file (downloaded in step 1) from the HAFM appliance CD-ROM or hard drive. Ensure the correct directory path and filename appear in the **File name** field and click **Save**.

The **New Firmware Description** dialog box displays.

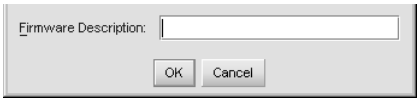


Figure 49: Firmware Description dialog box

7. Enter a description (up to 24 characters) for the new firmware version and click **OK**. The description should include the installation date and text that uniquely identify the firmware version.
8. A **Transfer Complete** message box displays indicating the new firmware version is stored on the HAFM appliance hard drive. Click **Close** to close the message box.
9. The new firmware version and associated description appear in the **Firmware Library** dialog box. Click **Close** to close the dialog box and return to the *Element Manager* application.
10. To send the firmware version to a switch, refer to "Download a Firmware Version to a Switch" on page 167.

Modify a Firmware Version Description

To modify the description of a switch firmware version in the library stored on the HAFM appliance hard drive:

1. Open the *HAFM* application. The View All - HAFM 8 main window displays.
2. Double-click the icon representing the switch for which the firmware version description will be modified. The **Hardware View** for the selected switch displays.
3. Choose **Maintenance > Firmware Library**. The Edge Switch 2/32 Firmware Library dialog box displays, as shown in Figure 47.
4. Select the firmware version to be modified and click **Modify**. The Modify Firmware Description dialog box displays, as shown in Figure 50.

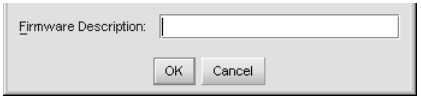


Figure 50: Modify Firmware Description

5. Enter a modified description (up to 24 characters) for the firmware version and click **OK**. It is recommended the description include the installation date and text that uniquely identifies the firmware version.
6. The new description for the firmware version displays in the Edge Switch 2/32 Firmware Library dialog box.
7. Click **Close**.

Delete a Firmware Version

To delete a switch firmware version from the library stored on the HAFM appliance hard drive:

1. Open the *HAFM* application. The View All - HAFM 8 main window displays.
2. Double-click the icon representing the switch from which the firmware version will be deleted. The **Hardware View** for the selected switch displays.
3. Choose **Maintenance > Firmware Library**. The Edge Switch 2/32 Firmware Library dialog box displays, as shown in Figure 47.
4. Select the firmware version to be deleted and click **Delete**. A confirmation dialog box displays.
5. Click **OK**. The selected firmware version is deleted from the Edge Switch 2/32 Firmware Library dialog box.
6. Click **Close**.

Download a Firmware Version to a Switch

This procedure downloads a selected firmware version from the HAFM appliance library to a switch managed by the open instance of the *Element Manager* application.

Note: When downloading a firmware version, follow all procedural information in the release notes or EC instructions that accompany the firmware version. This information supplements information in this general procedure.

To download a firmware version to a switch:

1. Notify the customer that a firmware version is to be downloaded to the switch. The switch resets during the firmware download, causing Fibre Channel links to momentarily drop and attached devices to log out and log back in. Data frames lost during switch reset must be retransmitted.
2. Open the *HAFM* application. The View All - HAFM 8 main window displays.
3. Before downloading firmware version XX.YY.ZZ to a switch, ensure version XX.YY.ZZ or higher of the *HAFM* application is running on the HAFM appliance.
   a. Choose **Help** > **About**. The **About** dialog box displays the *HAFM* application version. Click **OK** to close the dialog box.
   b. If required, install the correct version of the *HAFM* application ("Install or Upgrade Software" on page 175).
4. Double-click the icon representing the switch for which a firmware version is to be downloaded. The **Hardware View** for the selected switch displays.
5. As a precaution to preserve switch configuration information, perform the data collection procedure ("Collecting Maintenance Data" on page 151).
6. Choose **Maintenance** > **Firmware Library**. The **Firmware Library** dialog box displays.
7. Select the firmware version to be downloaded and click **Send**. The send function verifies existence of certain switch conditions before the download begins. If an error occurs, a message displays indicating the problem must be fixed before the firmware download. Conditions that terminate the process include:
   — The firmware version is being installed to the switch by another user.
   — The switch-to-HAFM appliance link fails or times out.

   If a problem occurs and a corresponding message displays, go to "MAP 0000: Start MAP" on page 29 to isolate the problem. If no error occurs, the **Send Firmware** confirmation box displays.
8. Click **Yes**. The **Send Firmware** dialog box displays.

   As the download begins, a `Writing data to Flash` message displays at the top of the dialog box followed by a `Sending Files` message. This message remains for a few moments as a progress bar travels across the dialog box to show percent completion of the download. As the download progresses, a `Writing data to FLASH` message displays. This message

remains as the progress bar continues to travel across the dialog box. The bar progresses to 100% when the last file is transmitted to the CTP card. The switch then performs an IPL, during which the switch-to-HAFM appliance link drops momentarily and the following occur at the *Element Manager* application:

— As the network connection drops, the **Status** table turns yellow, the **Status** field displays `No Link`, and the **State** field displays a reason message.

— In the HAFM Physical Map, the switch icon displays a gray square, indicating switch status is unknown.

— Illustrated FRUs in the **Hardware View** disappear, and appear again as the connection is re-established.

After the IPL, a `Send firmware complete` message displays.

9. Click **Close** to close the dialog box.
10. Click **Close**.

Manage Configuration Data

The *Element Manager* application provides maintenance options to back up, restore, or reset the configuration file stored in nonvolatile random-access memory (NV-RAM) on the switch CTP card. Configuration data in the file include:

- Identification data (switch name, description, and location).
- Port configuration data (port names, blocked states, extended distance settings).
- Operating parameters (buffer-to-buffer credit [BB_Credit] value, error-detect time-out value [E_D_TOV], resource allocation time-out value [R_A_TOV], switch priority, and preferred domain ID).
- SNMP configuration information, including trap recipients, community names, and write authorizations.
- Zoning configuration information, including the active zone set and default zone state.

Back Up the Configuration

To back up the switch configuration file to the HAFM appliance (c:\HafmData):

1. Open the *HAFM* application. The View All - HAFM 8 main window displays.
2. Double-click the icon representing the switch for which the configuration file will be backed up. The **Hardware View** for the selected switch displays.
3. Choose **Maintenance > Backup & Restore Configuration**. The **Backup and Restore Configuration** dialog box displays.
4. Click **Backup**. When the backup process finishes, a confirmation message displays.

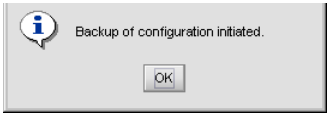


Figure 51: Backup Complete message

5. Click **OK** to close the dialog box and return to the **Hardware View**.

Restore the Configuration

To restore the switch configuration file from the HAFM appliance:

1. Notify the customer that the switch is to be set offline. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the switch and sets attached devices offline.
2. Set the switch offline ("Set Offline State" on page 160).
3. Open the *HAFM* application. The View All - HAFM 8 main window displays.
4. Double-click the icon representing the switch for which the configuration file will be restored. The **Hardware View** for the selected switch displays.
5. Choose **Maintenance > Backup & Restore Configuration**. The **Backup and Restore Configuration** dialog box displays.
6. Click **Restore**. A **Warning** message box displays.
7. Click **Yes**. When the restore process finishes, the **Restore Complete** message displays.
8. Click **OK** to close the dialog box and return to the **Hardware View**.

Reset Configuration Data

Note: This procedure resets the switch IP address to the default of 10.1.1.10 and may disrupt server-to-switch communication. All optional features are disabled.

To reset the switch data to the factory default settings:

1. Notify the customer the switch is to be set offline. Ensure the customer's system administrator quiesces Fibre Channel frame traffic through the switch and sets attached devices offline.
2. Set the switch offline ("Set Offline State" on page 160).
3. Open the *HAFM* application. The View All - HAFM 8 main window displays.
4. Double-click the icon representing the switch for which the configuration file will be reset to factory default settings. The **Hardware View** for the selected switch displays.
5. Choose **Maintenance > Reset Configuration**. The **Reset Configuration** dialog box displays.
6. Click **Reset**. When the reset process finishes, the dialog box closes and the application returns to the **Hardware View**.
7. The switch IP address resets to the default address of `10.1.1.10`.
   - If the configured IP address (prior to reset) was the same as the default address, the switch-to-HAFM appliance Ethernet link is not affected and the procedure is complete.
   - If the configured IP address (prior to reset) was not the same as the default address, the switch-to-HAFM appliance Ethernet link drops and HAFM appliance communication is lost. Continue to the next step.
8. To change the switch IP address and restart the HAFM appliance session, go to step 10.
9. To restart an HAFM appliance session using the default IP address of **10.1.1.10**:
   a. Close the Edge Switch 2/32 *Element Manager* application and return to *HAFM* application.
   b. A gray square with a yellow exclamation mark displays adjacent to the icon representing the reset switch, indicating the switch is not communicating with the HAFM appliance.

c. At the *HAFM* application, choose **Discover > Setup**. The Discover Setup dialog box displays, as shown in Figure 52.

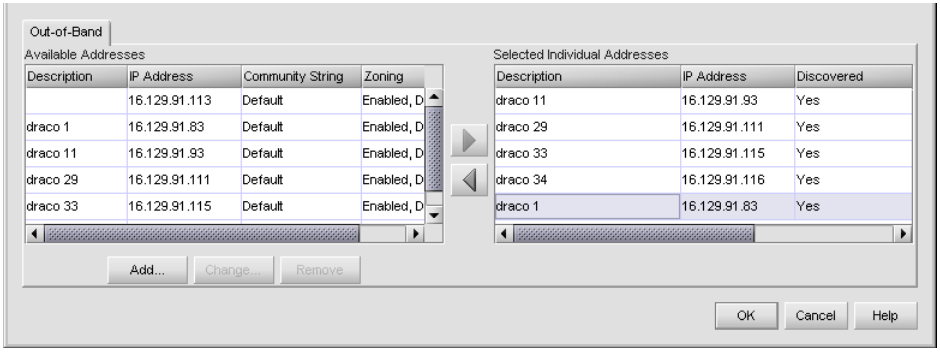


Figure 52: Discover Setup dialog box

d. Highlight the entry representing the reset switch in the **Available Addresses** window and click **Change**. The Domain Information dialog box displays, as shown in Figure 53.

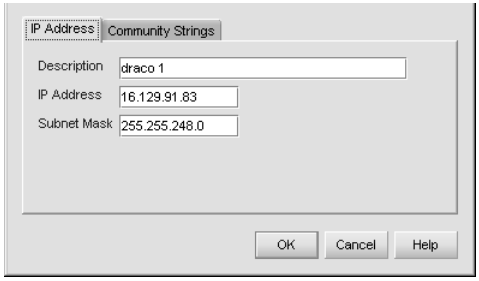


Figure 53: Domain Information dialog box

e. Enter `10.1.1.10` in the **IP Address** field and click **OK**. Entries at the Discover Setup dialog box reflect the new IP address.

f. At the Discover Setup dialog box, click **OK**. switch-to-HAFM appliance communication is restored and the procedure is complete.

10. Change the switch IP address and restart the HAFM appliance session as follows:

a. A gray square with a yellow exclamation mark displays adjacent to the icon representing the reset switch, indicating switch is not communicating with the HAFM appliance.

b. Delete the icon representing the reset switch. At the *HAFM* application, choose **Discover > Setup**. The Discover Setup dialog box displays, as shown in Figure 52.

c. Highlight the entry representing the reset switch in the **Available Addresses** window and click **Remove**.

d. At the Discover Setup dialog box, click **OK**. The switch is no longer defined to the management server.

e. Change a switch's IP address through the maintenance port at the rear of the switch. Refer to the *HP StorageWorks Edge Switch 2/32 Installation Guide* for information on configuring switch network information.

f. Identify the switch to the *HAFM* application. Refer to the *HP StorageWorks Edge Switch 2/32 Installation Guide* for information on identifying the switch to the *HAFM* application

g. Switch-to-HAFM appliance communication is restored and the procedure is complete.

Install or Upgrade Software

This section describes the procedure to install or upgrade the *HAFM* application to the HAFM appliance. The *HAFM* application includes the switch Element Manager and HAFM services applications.

The *HAFM* application shipped with the switch is provided on the HAFM Applications CD-ROM. Subsequent software versions for upgrading the switch are provided to customers through the HAFM Applications CD-ROM or through Hewlett-Packard's home page.

Note: When installing or upgrading a software version, follow all procedural information in the release notes or instructions that accompany the software version. This information supplements information in this general procedure.

To install or upgrade the *HAFM* application and associated applications to the HAFM appliance:

1. Log out of all *HAFM* application sessions (local and remote) and exit the *HAFM* application.
2. Obtain the new software version from the HP web site:

Note: The following path is subject to change.

---

   a. At the HAFM appliance or other personal computer (PC) with Internet access, open the HP web site. The uniform resource locator (URL) is: http://h18006.www1.hp.com/storage/saninfrastructure.html

---

Note: If required, obtain the customer-specific member name and password from the customer or next level of support.

---

   b. Follow links to HAFM software.
   c. Click the **HAFM Software Version XX.YY.ZZ** entry, where **XX.YY.ZZ** is the desired version. The Windows 2000 Save As dialog box displays.

d. Ensure the correct directory path is specified at the **Save in** field and the correct file is specified in the **File name** field. Click **Save**. The new HAFM version is downloaded and saved to the HAFM appliance or PC hard drive.

e. If the new HAFM version was downloaded to a PC (not the HAFM appliance), transfer the HAFM software version file to the HAFM appliance by CD-ROM or other electronic means.

3. Choose **Start > Run**. The Run dialog box displays, as shown in Figure 54.

Figure 54: Run dialog box

4. At the Run dialog box, select the directory path (hard drive or CD-ROM drive) and filename of the executable file (*HAFM_SERVERINSTALL.EXE*) using **Browse**. The directory path and filename display in the **Open** field.

5. Click **OK**. A series of message boxes displays as the *InstallAnywhere* application, as shown in Figure 55, prepares to install the *HAFM* application software, followed by the HP StorageWorks HA-Fabric Manager dialog box.

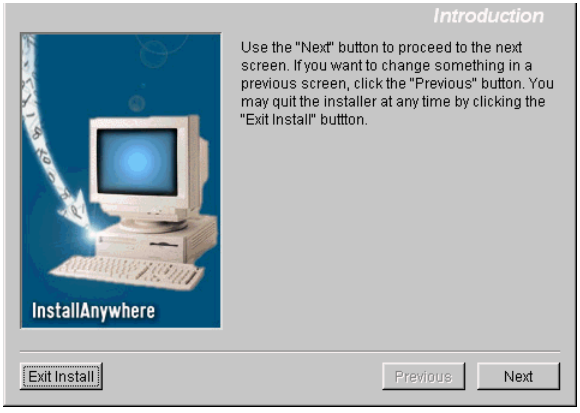


Figure 55: InstallAnywhere dialog box (Introduction)

6. Follow the online instructions for the *InstallAnywhere* program. Click **Next**, **Install**, or **Done** as appropriate.

7. Power off and reboot the HAFM appliance.
   a. Simultaneously press **Ctrl + Alt + Delete** to display the Windows 2000 Logon Information dialog box.
   b. Type the username and password and click **OK**. The **Windows 2000** desktop displays.

Note: If required, obtain the username and password from the customer or next level of support.

---

8. The *HAFM* application automatically opens and the HAFM 8 Log In dialog box displays.
9. Enter the HAFM appliance IP address in the **Network Address** field. If you are logging in to the local HAFM appliance, the HAFM appliance name is *localhost*.

   The default address that displays in the **Network Address** field is the address of the last server accessed. Click the HAFM appliance arrow to see the network addresses of all HAFM appliances that were accessed from the computer you are logged into.

   If you want to connect to an HAFM appliance that is not listed, enter the IP address in the **Network Address** field.
10. Enter your user name and password in the **User Name** and **Password** fields. User names and passwords are case-sensitive.
11. If you want your computer to save the login information, choose the **Save Password** option.
12. Click **Login**. The View All - HAFM 8 window displays.

Note: If required, obtain the username, password, and HAFM appliance name from the customer or next level of support.

FRU Removal and Replacement

4

This chapter describes the removal and replacement procedures (RRPs) for the HP StorageWorks Edge Switch 2/32 field-replaceable units (FRUs). Do not remove a FRU until a failure is isolated to that FRU. If fault isolation was not performed, see “MAP 0000: Start MAP” on page 29.

Procedural Notes

Note the following:

1. Read the removal and replacement procedures (RRPs) for that FRU before removing the FRU.
2. Follow all **WARNING** and **CAUTION** statements and statements in the preface of this manual.
3. After completing a FRU replacement, clear the event code reporting the failure and the event code reporting the recovery from the switch **Event Log** (at the HAFM appliance). Extinguish the amber system error (**ERR**) light-emitting diode (LED) at the switch front panel.

Remove and Replace FRUs

This section describes procedures to remove and replace concurrent switch FRUs, along with tools required to perform each procedure. Concurrent FRUs are removed and replaced while the switch is powered on and operational.

Table 20 lists concurrent FRUs that are removed and replaced while the switch is powered on and operational. The table also lists ESD precautions (yes or no) for each FRU, and references the page number of the removal and replacement procedure.

Table 20: Concurrent FRUs

Concurrent FRU Name	ESD Precaution Requirement
Small form factor pluggable (SFP) optical transceiver	No
Power supply	No
Cooling fan	No

RRP: SFP Optical Transceiver

Use the following procedures to remove or replace an SFP optical transceiver from the front of the switch chassis. A list of tools required is provided.

Tools Required

The following tools are required to perform these procedures.

- Protective cap (provided with the fiber-optic jumper cable).
- Loopback plug (provided with the switch).
- Fiber-optic cleaning kit.

Removal

To remove an SFP optical transceiver:

1. Notify the customer that the port with the defective transceiver will be blocked. Ensure the customer's system administrator sets the attached device offline.
2. Identify the defective port transceiver from:
   - The illuminated amber LED adjacent to the port.
   - At the EWS interface, failure information associated with the port at the **Port Properties** page of the **View** panel.
   - At the HAFM appliance, failure information associated with the port at the **Hardware View**, **Port List View**, or **Port Properties** dialog box.
3. Block communication to the port ("Block and Unblock Ports" on page 161).
4. Disconnect the fiber-optic jumper cable from the port:
   a. Pull the keyed LC connector free from the port's optical transceiver.
   b. Place a protective cap over the jumper cable connector.
5. The optical transceiver has a wire locking bale to secure the transceiver in the port receptacle and to assist in removal. The locking bale rotates up or down, depending on the transceiver manufacturer and port location (top row, odd-numbered ports **1** through **31**, or bottom row, even-numbered ports **0** through **30**).
   a. Disengage the locking mechanism by rotating the wire locking bale up or down 90 degrees.

b. Grasp the wire locking bale and pull the transceiver from the port receptacle.

6. Perform one of the following to inspect the **Event Log**:

— If at a Web browser connected to the EWS interface, click the **Log** tab at the **Monitor** panel. The **Event Log** displays. An event code **513** (SFP optics hot-removal completed) displays in the log.

— If at the HAFM appliance, open the **Hardware View** and choose **Logs > Event Log**. The **Event Log** displays. An event code **513** (SFP optics hot-removal completed) displays in the log.

Replacement

To replace an SFP optical transceiver:

1. Remove the replacement transceiver from its packaging.
2. Insert the transceiver into the port receptacle, then engage the locking mechanism by rotating the wire locking bale up or down 90 degrees.
3. Perform an external loopback test on the port. Refer to "Perform Loopback Tests" on page 146 for instructions. If the test fails, go to "MAP 0000: Start MAP" on page 29 to isolate the problem.
4. Reconnect the fiber-optic jumper cable:
   a. Remove the protective cap from the cable connector and the protective plug from the port's optical transceiver. Store the cap and plug in a suitable location for safekeeping.
   b. Clean the jumper cable and transceiver connectors. Refer to "Clean Fiber-Optic Components" on page 153 for instructions.
   c. Insert the keyed LC cable connector into the port's optical transceiver.
5. Ensure the amber LED adjacent to the port transceiver is extinguished. If the amber LED is illuminated, go to "MAP 0000: Start MAP" on page 29 to isolate the problem.
6. Perform one of the following to inspect the **Event Log**:

— If at a Web browser connected to the EWS interface, click the **Log** tab at the **Monitor** panel. The **Event Log** displays. Ensure an event code **510** (SFP optics hot-insertion initiated) displays. If the event code does not appear in the log, go to "MAP 0000: Start MAP" on page 29 to isolate the problem.

— If at the HAFM appliance, open the **Hardware View**, choose **Logs > Event Log**. The **Event Log** displays. Ensure an event code **510** (SFP optics hot-insertion initiated) displays. If the event code does not appear in the log, go to "MAP 0000: Start MAP" on page 29 to isolate the problem.

7. Perform one of the following to verify port operation:

   If at a Web browser connected to the EWS interface, open the **Switch** tab at the **View** panel and:

   a. Ensure no amber LEDs illuminate that indicate a port failure.

   b. Click the graphic representing the port with the replacement transceiver to open the **Port Properties** tab. Verify port and port technology information is correct.

   c. If a problem is indicated, go to "MAP 0000: Start MAP" on page 29 to isolate the problem.

   If at the HAFM appliance, open the **Hardware View** and:

   a. Ensure no alert symbols appear that indicate a port failure (yellow triangle or red diamond).

   b. Double-click the graphic representing the port with the replacement transceiver to open the **Port Properties** dialog box. Verify port information is correct.

   c. Right-click the graphic representing the port with the replacement transceiver and select **Port Technology** from the menu. The **Port Technology** dialog box displays. Verify port technology information is correct.

   d. If a problem is indicated, go to "MAP 0000: Start MAP" on page 29 to isolate the problem.

8. Restore communication to the port with the replacement transceiver as directed by the customer. Refer to "Block and Unblock Ports" on page 161 for instructions. Inform the customer the port is available.

9. Perform one of the following to clear the system error (**ERR**) LED on the switch front bezel:

   — If at a Web browser connected to the EWS interface, click the **Log** tab at the **Monitor** panel. The **Event Log** displays. Click **Clear System Error Light**.

— If at the HAFM appliance, open the **Hardware View**, right-click the front panel bezel graphic (away from a FRU) to open a menu. Click the **Clear System Error Light** menu selection.

"MAP 0000: Start MAP on page 29" "MAP 0000: Start MAP on page 29"

RRP: Cooling Fan

Use the following procedures to remove or replace a cooling fan FRU from the rear of the switch. No tools are required.

Removal

To remove a cooling fan:

1. Identify the defective cooling fan from the illuminated amber LED on the fan or failure information at the HAFM appliance **Hardware View**.
2. Loosen the fan retaining screw in the upper right corner of the fan. The retaining screw is captive and will remain in the fan assembly.
3. Grasp the fan handle and pull the fan FRU out of the chassis.

Replacement

To replace a cooling fan:

1. Remove the replacement cooling fan FRU from its shipping container.
2. Inspect the rear of the fan for bent or broken connector pins. If any pins are damaged, obtain a new fan.
3. Position the fan FRU with its retaining screw at the upper right corner (the fan cannot be inserted in any other position).
4. Push the fan FRU into the chassis to engage the connector pins. Ensure that the fan FRU faceplate is flush with the chassis.
5. Engage the screw threads and lightly tighten the screw. Over-tightening the screw may damage the FRU or chassis.
6. Inspect the fan FRU to ensure that the amber LED is extinguished. If the amber LED is illuminated, go to "MAP 0000: Start MAP" on page 29 to isolate the problem.
7. At the HAFM appliance **Hardware View**, click **Event Log** from the **Logs** icon. The **Event Log** window displays. Ensure one of the following event codes displays in the log:

   310 to 315 — *N*th cooling fan has recovered, where *N* is first to fourth (fan).

RRP: Power Supply

Use the following procedures to remove or replace a power supply from the rear of the switch. No tools are required.

Removal

To remove a power supply:

1. Identify the defective power supply from the extinguished green LED at the switch or failure information at the HAFM appliance **Hardware View**.
2. Turn off the power switch on the power supply.
3. Disconnect the AC power cord from the power supply.
4. Rotate the power lockout lever to the right to expose the black plastic latch lever.
5. Pull the latch lever down to the horizontal position.

   The power supply will disengage and back out about 1/4 inch when the lever is horizontal.
6. Use the latch lever to pull the power supply out of the chassis. Support the power supply as it exits the chassis.

WARNING: To prevent electric shock, do not reach into nonvisible areas of a switch while the switch is connected to primary facility power.

Replacement

To replace a power supply:

1. Remove the replacement power supply from its shipping container.
2. Inspect the rear of the power supply for bent or broken connector pins. If any pins are damaged, obtain a new power supply.
3. Ensure that the power switch on the power supply is turned off, the power lockout lever is rotated to the right, covering the AC connector, and the black plastic latch lever is completely down in the horizontal position.
4. Insert the power supply into the chassis until it stops.

5. Raise the black plastic latch lever to the vertical position.

   The power supply cams into its seated position in the chassis.

6. Rotate the power lockout lever to the left to cover the plastic lever and expose the AC connector.
7. Verifying that the power switch is off, connect the AC power cord to the power supply and to a facility power source.
8. Turn on the power switch.
9. Inspect the power supply to ensure that the green LED is illuminated. If the green LED is extinguished, go to"MAP 0000: Start MAP" on page 29 to isolate the problem.
10. At the HAFM appliance **Hardware View**, select **Event Log** from the **Logs** icon. The Event Log displays. Ensure the following event codes display in the log:
    - **203 —** Power supply AC voltage recovery.
    - **204 —** Power supply DC voltage recovery.
11. At the HAFM appliance **Hardware View**, observe the power supply graphic and ensure no alert symbols display that indicate a failure (yellow triangle or red diamond). If a problem is indicated, go to "MAP 0000: Start MAP" on page 29 to isolate the problem.
12. Perform the data collection procedure (refer to "Collecting Maintenance Data" on page 151).
13. Clear the switch system error (**ERR**) LED:
    a. At the HAFM appliance **Hardware View**, right-click the front panel bezel graphic (away from a FRU) to open a pop-up menu.

Click the **Clear System Error Light** menu selection.

Illustrated Parts Breakdown

5

This chapter provides an illustrated parts breakdown for the HP StorageWorks Edge Switch 2/32 field-replaceable units (FRUs). Exploded-view assembly drawings are provided for:

- Front-accessible FRUs.
- Rear-accessible FRUs.
- Miscellaneous parts.

Exploded-view illustrations portray the switch disassembly sequence. Illustrated FRUs are numerically keyed to associated tabular parts lists. The parts lists also include part numbers, descriptions, and quantities.

Front-Accessible FRUs

The front-accessible switch FRUs are illustrated and described in Figure 56 and Table 21. The table includes reference numbers to the figure, part numbers, descriptions, and quantities.

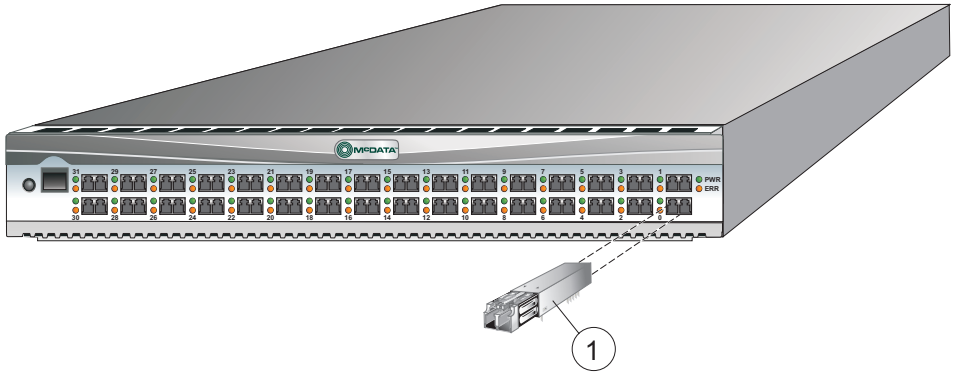


Figure 56: Front-accessible FRUs

Table 21: Front-Accessible FRU Parts List

Ref.	Part Number	Description	Qty.
N/A	286810-B21	Base assembly, Edge Switch 2/32, without optics	N/A
❶	300834-B21	Transceiver, optical, SFP, shortwave laser, LC connector, 2.125 Gb/s	0 to 32
❶	300835-B21	Transceiver, optical, SFP, longwave laser, LC connector, 10 km, 2.125 Gb/s	0 to 32
❶	300836-B21	Transceiver, optical, SFP, longwave laser, LC connector, 35 km, 2.125 Gb/s	0 to 32

Rear-Accessible FRUs

The FRUs and their part numbers differ between the two packaging systems for the switch. Use care when selecting a part number to order for replacement purposes, to ensure that the part number matches the switch for which it is intended.

The rear-accessible switch FRUs are illustrated and described in Figure 57 and Table 22. The table includes reference numbers to the figure, part numbers, descriptions, and quantities.

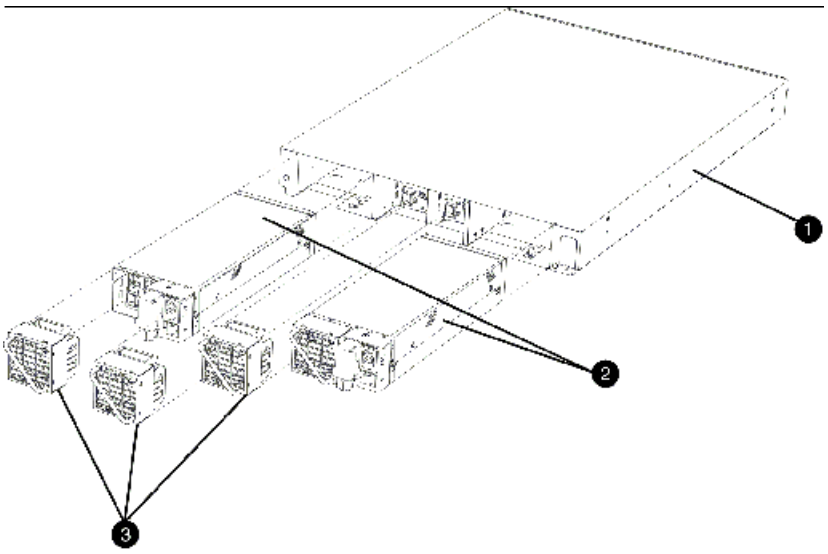


Figure 57: Rear-Accessible FRUs

Table 22: Rear-Accessible FRU Parts List

Ref.	Part Number	Description	Qty.
❶	292008-001	Base assembly, Edge Switch 2/32, without optics	Reference
❷	292012-001	Power supply assembly (includes one cooling fan, P/N 292010-001)	2
❸	292010-001	Fan, cooling	4

Miscellaneous Parts

Table 23 is a list of miscellaneous parts.

Table 23: Miscellaneous Parts

Part Number	Description	Qty.
254145-001	Plug, loopback, LC connector, multimode, 50/125 micron (#1148)	1
254146-001	Plug, loopback, LC connector, singlemode, 9/125 micron (#1149)	1
254144-001	Cable, null modem, DB9F-DB9F connector	1
254143-001	Cable, Ethernet, 10-foot	1

Messages

This appendix lists information and error messages that appear in pop-up message boxes at the HP StorageWorks HA-Fabric Manager (HAFM) application and the Edge Switch 2/32 *Element Manager* application.

HAFM Application Messages

This section lists *HAFM* application information and error messages in alphabetical order.

Table 24: HAFM application messages

Message	Description	Action
A zone must have at least one zone member.	When creating a new zone, one or more zone members must be added.	Add one or more zone members to the new zone.
A zone set must have at least one zone.	When creating a new zone set, one or more zones must be added.	Add one or more zones to the new zone set.
All zone and zone set names must be unique.	When creating a new zone or zone set, the name must be unique.	Choose a unique name for the new zone or zone set.
All zone members are logged.	An attempt was made to display all zone members not logged in using the **Zone Set** tab, but all members are logged in.	Information message–no action required.
An HAFM application session is already active from this workstation.	Only one instance of the *HAFM* application is allowed to be open per remote workstation.	Close all but one of the *HAFM* application sessions.
Are you sure you want to delete this network address?	The currently selected network address will be deleted.	Click **Yes** to delete or **No** to cancel.
Are you sure you want to delete this nickname?	The selected nickname will be deleted from the list of nickname definitions.	Click **Yes** to delete the nickname or **No** to cancel the operation.
Are you sure you want to delete this product?	The selected product will be deleted from the list of product definitions.	Click **Yes** to delete the product or **No** to cancel the operation.
Are you sure you want to delete this user?	The selected user will be deleted from the list of user definitions.	Click **Yes** to delete the user or **No** to cancel the operation.
Are you sure you want to delete this zone?	The selected zone will be deleted from the zone library.	Click **Yes** to delete the zone or **No** to cancel the operation.

Table 24: HAFM application messages (Continued)

Message	Description	Action
Are you sure you want to overwrite this zone set?	The selected zone set will be overwritten in the zoning library.	Click **Yes** to overwrite or **No** to cancel.
Are you sure you want to remove all members from this zone?	All members will be deleted from the selected zone.	Click **Yes** to delete the members or **No** to cancel the operation.
Cannot add a switch to a zone.	The device that you are attempting to add to the zone is a switch, which cannot be added to a zone.	Specify the port number or corresponding World Wide Name (WWN) for the device you want to add to the zone.
Cannot connect to HAFM appliance.	The *HAFM* application at a remote workstation could not connect to the HAFM appliance.	Verify the HAFM appliance internet protocol (IP) address is valid.
Cannot delete product.	The selected product cannot be deleted.	Verify the HAFM appliance-to-product link is up. If the link is up, the HAFM appliance may be busy. Another Element Manager instance may be open. The user may not have permission to delete the product.
Cannot disable Fabric Binding while Enterprise Fabric Mode is active.	The user attempted to disable fabric binding through the Fabric Binding dialog box, but Enterprise Fabric Mode was enabled.	Disable Enterprise Fabric Mode through the Enterprise Fabric Mode dialog box before disabling fabric binding.
Cannot display route on a one switch fabric.	The user cannot show routes between end devices in a fabric when configuring **Show Route** from the **Fabrics** menu.	This error displays when attempting to show routes on a fabric with only one switch. Configure the Show Route option only for a multiswitch fabric.
Cannot display route. Device is not a member of a zone in the active zone set.	The user cannot show the route for a device that is not a member of a zone in the active zone set.	Enable the default zone or activate the zone for the device before attempting to show the route.

Table 24: HAFM application messages (Continued)

Message	Description	Action
Cannot display route. Error 9.	An internal error occurred while trying to show routes.	Retry the operation. If the condition persists, contact support personnel and report the problem.
Cannot display route. No active zone enabled.	You cannot show the route through a fabric with no active zone.	Enable the default zone or activate a zone set before attempting to show the route.
Cannot display route. All switches in route must be managed by the same server.	You cannot show the route through a fabric that has switches or directors that are managed by a different HAFM appliance.	This route cannot be shown unless all Edge Switches and Directors in the route are managed by this HAFM appliance.
Cannot display route. All switches in route must support routing.	You cannot show the route through a fabric that has switches or directors which do not support routing.	The route must contain only Directors or Edge Switches.
Cannot have spaces in field.	Spaces are not allowed as part of the entry for this field.	Delete spaces from the field entry.
Cannot modify a zone set with an invalid name. Rename zone set and try again.	A zone set must have a valid name to be modified.	Assign a valid name to the zone set, then click **Modify**.
Cannot modify a zone with an invalid name. Rename zone and try again.	A zone must have a valid name to be modified.	Assign a valid name to the zone, then click **Modify**.
Cannot modify product.	The selected product cannot be modified.	Verify the HAFM appliance-to-product link is up. If the link is up, the HAFM appliance may be busy. Another Element Manager instance may be open. The user may not have permission to modify the product.

Table 24: HAFM application messages (Continued)

Message	Description	Action
Cannot perform operation. Fabric is unknown.	This message displays if no switches in the fabric are connected to the HAFM appliance.	Ensure at least one fabric-attached switch or director has an Ethernet connection to the HAFM appliance and retry the operation.
Cannot perform operation. The list of attached nodes is unavailable.	This message displays when attached nodes are unavailable and the user attempts to modify a zone or create a new zone.	Verify an attached node is available and retry the operation.
Cannot retrieve current SNMP configuration.	The current SNMP configuration could not be retrieved.	Try again. If the problem persists, contact the next level of support.
Cannot save current SNMP configuration.	The current SNMP configuration could not be saved.	Try again. If the problem persists, contact the next level of support.
Cannot set write authorization without defining a community name.	An SNMP community name is not configured.	Enter a valid community name in the **Configure SNMP** dialog box.
Cannot show zoning library. No fabric exists.	The user cannot show the zoning library if no fabric exists. A Director or Edge Switch must be identified to the *HAFM* application for a fabric to exist.	Identify a Director or Edge Switch to the *HAFM* application from the **New Product** dialog box.
Click **OK** to remove all contents from log.	This action deletes all contents from the selected log.	Click **OK** to delete the log contents or **Cancel** to cancel the operation.
Connection to HAFM appliance lost.	The connection to the remote HAFM appliance was lost.	Log in to the HAFM appliance again through the **HAFM Login** dialog box.
Connection to HAFM appliance lost. Click **OK** to exit application.	The *HAFM* application at a remote workstation lost the network connection to the HAFM appliance.	Start the *HAFM* application to connect to the HAFM appliance.

Table 24: HAFM application messages (Continued)

Message	Description	Action
Could not export log to file.	A log file input/output (I/O) error occurred and the file could not be saved to the specified destination. The disk may be full or write protected.	If the disk is full, use another disk. If the disk is write protected, change the write-protect properties or use another disk.
Default zoning is not supported in Open Fabric Mode.	A default zone cannot be enabled when the switches in a fabric are set to Open Fabric mode.	Change the setting from Open Fabric mode to Homogeneous mode and retry the default zoning operation.
Device is not a member of a zone in the active zone set.	The selected device is not a member of a zone in the active zone set and cannot communicate with the other device in the route.	Enable the default zone or activate a zone set containing the member before attempting to show the route.
Download complete. Click **OK** and start the HAFM.	Download of the *HAFM* and *Element Manager* applications is complete.	Start the *HAFM* application to continue.
Duplicate community names require identical write authorizations.	If configuring two communities with identical names, they must also have identical write authorizations.	Verify that both communities with the same name have the same write authorizations.
Duplicate Fabric Name.	The specified fabric name already exists.	Choose another name for the fabric.
Duplicate name in zoning configuration. All zone and zone set names must be unique.	Every name in the zoning library must be unique.	Modify (to make it unique) or delete the duplicate name.
Duplicate nickname in nickname configuration.	Duplicate nicknames cannot be configured.	Modify the selected nickname to make it unique.
Duplicate World-Wide Name in nickname configuration.	A world-wide name can be associated with only one nickname.	Modify (to make it unique) or delete the selected world-wide name.
Duplicate zone in zone set configuration.	More than one instance of a zone is defined in a zone set.	Delete one of the duplicate zones from the zone set.

Table 24: HAFM application messages (Continued)

Message	Description	Action
Duplicate zone member in zone configuration.	More than one instance of a zone member is defined in a zone.	Delete one of the duplicate zone members from the zone.
Element Manager instance is currently open.	A product cannot be deleted while an instance of the *Element Manager* application is open.	Close the *Element Manager* application, then delete the product.
Enabling this zone set will replace the currently active zone set. Do you want to continue?	Only one zone set can be active. By enabling the selected zone set, the active zone set will be replaced.	Click **OK** to continue or **Cancel** to end the operation.
Enterprise Fabrics feature not installed. Please contact your sales representative.	A user selected Fabric Binding or Enterprise Fabric Mode from the **Fabrics** menu. These selections are not enabled because the optional SANtegrity Binding feature is not installed.	Install the optional SANtegrity Binding feature to use Fabric Binding or enable Enterprise Fabric Mode.
Error creating zone.	The *HAFM* application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
Error creating zone set.	The *HAFM* application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
Error deleting zone.	The *HAFM* application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
Error deleting zone set.	The *HAFM* application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
Error reading log file.	The *HAFM* application encountered an error while trying to read the log.	Try the operation again. If the problem persists, contact the next level of support.

Table 24: HAFM application messages (Continued)

Message	Description	Action
Error removing zone or zone member.	The *HAFM* application encountered an internal error.	Try the operation again. If the problem persists, contact the next level of support.
Error transferring files < message >.	An error occurred while transferring files from the PC hard drive to the *HAFM* application. The message varies, depending on the problem.	Try the file transfer operation again. If the problem persists, contact the next level of support.
Fabric Log will be lost once the fabric unpersists. Do you want to continue?	When you unpersist a fabric, the corresponding Fabric Log is deleted.	Click Yes to unpersist the fabric or No to cancel the operation.
Fabric not persisted.	The user attempted to refresh or clear the Fabric Log after a fabric was unpersisted. When you unpersist a fabric, the corresponding Fabric Log is deleted.	Click **OK** to continue. Ensure the fabric is persisted before attempting to refresh or clear the Fabric Log.
Field cannot be blank.	The data field requires an entry and cannot be left blank.	Enter appropriate information in the data field.
Field has exceeded maximum number of characters.	The maximum number of data entry characters allowed in the field was exceeded.	Enter the information using the proscribed number of characters.
File transfer aborted.	The user aborted the file transfer process.	Verify the file transfer is to be aborted, then click **OK** to continue.
HAFM management session is already active from this workstation.	An HAFM management session is open and active at this workstation.	A workstation can have only one active HAFM management session.
HAFM error <error number 1 through 8 >.	The *HAFM* application encountered an internal error (**1** through **8** inclusive) and cannot continue operation.	Contact the next level of support to report the problem.

Table 24: HAFM application messages (Continued)

Message	Description	Action
HAFM appliance is shutting down. Connection will be terminated.	The *HAFM* application is closing and terminating communication with the attached product.	Reboot the HAFM appliance. If the problem persists, contact the next level of support.
HAFM appliance could not log you on. Verify your username and password.	The incorrect username and/or password (both case sensitive) were used while attempting to login to the *HAFM* application.	Verify the user name and password with the customer's network administrator and retry the operation.
HAFM appliance is shutting down. Connection will be terminated.	The *HAFM* application is closing and terminating communication with the attached product.	Reboot the HAFM appliance. If the problem persists, contact the next level of support.
HAFM session is already active from this workstation.	An HAFM session already exists on the current workstation.	A workstation can have only one active HAFM session.
HP SANtegrity binding feature not installed. Please contact your sales representative.	A user selected **Fabric Binding** or **Enterprise Fabric Mode** from the **Fabrics** menu. These selections are not enabled because the optional SANtegrity binding feature is not installed.	Install the optional SANtegrity binding feature to use Fabric Binding or enable **Enterprise Fabric Mode**.
Invalid character in field.	An invalid character was entered in the data field.	Remove invalid characters from the entry.
Invalid HAFM appliance address.	The IP address specified for the HAFM appliance is unknown to the domain name server (invalid).	Verify and enter a valid HAFM appliance IP address.
Invalid name.	One of the following invalid names was used: CON, AUX, COM1, COM2, COM3, COM4, COM5, COM6, COM7, COM8, COM9, LPT1, LPT2, LPT3, LPT4, LPT5, LPT6, LPT7, LPT8, LPT9, NUL, or PRN.	Select a valid name and retry the operation.

Table 24: HAFM application messages (Continued)

Message	Description	Action
Invalid network address.	The IP address specified for the product is unknown to the domain name server (invalid).	Verify and enter a valid product IP address.
Invalid port number. Valid ports are (0-< nn >).	The user has specified an invalid port number.	Specify a valid port number, in the range 0 to the maximum number of ports on the product minus one. For example, for a switch with 32 ports, the valid port range is 0 to 31.
Invalid product selection.	At the New Product dialog box, an invalid product was selected.	Select a valid product and retry the operation.
Invalid request.	Three conditions result in this message: ■ The user tried to add or modify a product from **Product View** and the network (IP) address is already in use. Network addresses must be unique. ■ The user tried to create a new user with a user name that already exists. User names must be unique. ■ The user tried to delete default Administrator user. The default Administrator user cannot be deleted.	Select the action that is appropriate to the activity that caused the error: ■ Network address: Specify a unique network (IP) address for the product. ■ User name: Specify a unique user name for the new user ID. ■ Do not delete the default Administrator user.
Invalid UDP port number.	The specified user datagram protocol (UDP) port number is invalid. The number must be an integer from 1 through 65535 inclusive.	Verify and enter a valid UDP port number.

Table 24: HAFM application messages (Continued)

Message	Description	Action
Invalid World-Wide Name or nickname.	The specified world-wide name format is invalid. The valid format is eight two-digit hexadecimal numbers separated by colons (xx:xx:xx:xx:xx:xx:xx:xx).	Retry the operation using a valid WWN or nickname.
Invalid World-Wide Name. Valid WWN format is xx:xx:xx:xx:xx:xx:xx:xx.	The specified world-wide name format is invalid. The valid format is eight two-digit hexadecimal numbers separated by colons (xx:xx:xx:xx:xx:xx:xx:xx)	Retry the operation using a valid WWN format.
Invalid zone in zone set.	The defined zone no longer exists and is invalid.	Retry the operation using a valid zone.
Limit exceeded.	The user cannot add a new product or user to the *HAFM* application if the maximum number of that resource exists on the system.	Delete products or users from the system before attempting to add new ones.
Management session is already active from this workstation.	An instance of the *HAFM* application is already open at this workstation.	Close the previous session of the *HAFM* application before starting a new one.
No address selected.	The user cannot complete the operation because an address has not been selected.	Select an address and retry the operation.
No attached nodes selected.	An operation was attempted without an attached node selected.	Select an attached node and retry the operation.
No HAFM appliance specified.	An HAFM appliance is not defined to the *HAFM* application.	At the HAFM 8 Log In screen, type a server name in the **HAFM appliance** field and click **Login**.
No nickname selected.	No nickname was selected when the command was attempted.	Select a nickname and retry the operation.

Table 24: HAFM application messages (Continued)

Message	Description	Action
No Element Managers installed.	No Director or Edge Switch *Element Manager* application is installed on this workstation.	Install the appropriate Element Manager to this workstation.
No routing information available.	No information is available for the route selected.	Select a different route and retry the operation.
No user selected.	A user was not selected when the command was attempted.	Select a user and retry the operation.
No zone member selected.	A zoning operation was attempted without a zone member selected.	Select a zone member and retry the operation.
No zone selected.	A zoning operation was attempted without a zone selected.	Select a zone and retry the operation.
No zone selected or zone no longer exists.	A zoning operation was attempted without a zone selected, or the zone selected no longer exists in the fabric.	Select a zone and retry the operation.
No zone set active.	A zone set cannot be deactivated if there are no active zones.	Informational message only-no action is required.
No zone set selected.	A zoning operation was attempted without a zone set selected.	Select a zone set and retry the operation.
No zone set selected or zone set no longer exists.	A zoning operation was attempted without a zone set selected, or the zone set you selected no longer exists in the fabric.	Select a zone set and retry the operation.
Only attached nodes can be displayed in this mode.	Users cannot display unused ports when adding ports by world-wide name.	Change the add criteria to **Add by Port**.

Table 24: HAFM application messages (Continued)

Message	Description	Action
Password and confirmation don't match.	Entries in the password field and confirmation password field do not match. The entries are case sensitive and must be the same.	Enter the password and confirmation password again.
Remote session support has been disabled.	The connection between the specified remote workstation and the HAFM appliance was disallowed.	Consult with the customer's network administrator to determine if the workstation entry should be modified at the **Session Options** dialog box.
Remote sessions are not allowed from this network address.	Only IP addresses of remote workstations specified at the **Session Options** dialog box are allowed to connect to the HAFM appliance.	Consult with the customer's network administrator to determine if the IP address is to be configured for remote sessions.
Resource is unavailable.	The specified operation cannot be performed because the product is unavailable.	Verify the HAFM appliance-to-product link is up. If the link is up, the HAFM appliance may be busy. Retry the operation later.
Select alias to add to zone.	An alias was not selected before clicking **Add**.	Choose an alias before clicking **Add**.
Selection is not a World-Wide Name.	The selection made is not a world-wide name.	Select a valid world-wide name before performing this operation.
Server shutting down.	The *HAFM* application is closing and terminating communication with the attached product.	Reboot the HAFM appliance. If the problem persists, contact the next level of support.
SNMP trap address not defined.	If an SNMP community name is defined, a corresponding SNMP trap recipient address must also be defined.	Enter a corresponding SNMP trap recipient address.

Table 24: HAFM application messages (Continued)

Message	Description	Action
The Administrator user cannot be deleted.	The Administrator user is permanent and cannot be deleted from the **Configure Users** dialog box.	Informational message only-no action is required.
The Domain ID was not accepted. The World Wide Name and Domain ID must be unique in the Fabric Membership List.	A user attempted to add a Director or Edge Switch to the fabric membership list through the Fabric Binding option (SANtegrity Binding feature), but a product already exists in the fabric with the same domain ID.	Enter a unique domain ID for the switch in the **Add Detached Switch** dialog box.
The HAFM appliance is busy processing a request from another Element Manager.	The HAFM appliance is processing a request from another instance of an *Element Manager* application, and cannot perform the requested operation.	Wait until the process completes, then retry the operation.
The link to the managed product is not available.	The Ethernet connection between the HAFM appliance and managed product is down or unavailable.	Establish and verify the network connection.
The maximum number of members has already been configured.	The maximum number of zone members that can be defined to the application was reached.	Delete an existing zone member before adding a new zone member.
The maximum number of nicknames has already been configured.	The maximum number of nicknames that can be defined to the *HAFM* application was reached.	Delete an existing nickname before adding a new nickname.
The maximum number of open products has already been reached.	The maximum number of open products allowed was reached.	Close an Element Manager session (existing open product) before opening a new session.

Table 24: HAFM application messages (Continued)

Message	Description	Action
The maximum number of products has already been configured.	The number of managed HA Fabric Directors and Edge Switches (48) that can be defined to the *HAFM* application was reached.	Delete an existing product before adding a new product.
The maximum number of products of this type has already been configured.	The number of HA Fabric Directors and Edge Switches of this type (48) that can be defined to the *HAFM* application was reached.	Delete an existing product of this type before adding a new product.
The maximum number of remote network addresses has already been configured.	A maximum of four IP addresses for remote workstations can be configured at the **Session Options** dialog box. That number was reached.	Delete an existing IP address before adding a new IP address.
The maximum number of HAFM application sessions has been reached.	A maximum of eight concurrent remote management sessions can be configured at the **Session Options** dialog box. The specified number was reached.	Increase the number of remote sessions allowed (if less than eight), or terminate a session before attempting to initiate a new session.
The maximum number of HAFM appliance network addresses has already been configured.	The number of HAFM appliance IP addresses that can be defined to the *HAFM* application was reached.	Delete an existing IP address before adding a new address.
The maximum number of users has already been configured.	The number of users (16) that can be defined to the *HAFM* application was reached.	Delete an existing user before adding a new user.
The maximum number of zones allowed has already been configured.	The maximum number of zones that can be defined was reached.	Delete an existing zone before adding a new zone.
The maximum number of zone sets has already been configured.	The maximum number of zone sets that can be defined was reached.	Delete an existing zone set before adding a new zone set.

Table 24: HAFM application messages (Continued)

Message	Description	Action
The maximum number of zones per zone set has already been configured.	The maximum number of zones that can be defined in a zone set was reached.	Delete an existing zone before adding a new zone to the zone set.
The nickname does not exist.	The entered nickname does not exist in the fabric.	Configure the nickname to the appropriate product or select an existing nickname.
The nickname is already assigned. Either use a different name or do not save the name as a nickname.	The entered nickname already exists in the fabric. Each nickname must be unique.	Define a different nickname.
The software version on this HAFM appliance is not compatible with the version on the remote HAFM appliance.	A remote HAFM appliance connecting to the HAFM appliance must be running the same software version to log in.	Upgrade the software version on the downlevel HAFM appliance.
The zoning library conversion must be completed before continuing.	The zoning library conversion is incomplete and the requested operation cannot continue.	Complete the zoning library conversion, then retry the operation.
This fabric log is no longer valid because the fabric has been unpersisted.	The selected Fabric Log is no longer available because the fabric was unpersisted.	To start a new log for the fabric, persist the fabric through the **Persist Fabric** dialog box.
This network address has already been assigned.	The specified IP address was assigned and configured. A unique address must be assigned.	Consult with the customer's network administrator to determine a new IP address to be assigned and configured.
This product is not managed by this HAFM appliance.	The product selected is not managed by this HAFM appliance.	Select a product managed by this HAFM appliance or go to the HAFM appliance that manages the affected product.

Table 24: HAFM application messages (Continued)

Message	Description	Action
This switch is currently part of this fabric and cannot be removed from the Fabric Membership List. Isolate the switch from the fabric prior to removing it from the Fabric Membership List.	A user attempted to remove a Director or Edge Switch from the fabric membership list using the Fabric Binding option, but the Director or Edge Switch is still part of the fabric.	Remove the director or switch from the fabric by setting the product offline or blocking the E_Port connection.
This user name has already been assigned.	The specified user name is already assigned and configured.	Modify (to make it unique) or delete the duplicate name.
This World Wide Name was not accepted. The World Wide Name and Domain ID must be unique in the Fabric Membership List.	A user attempted to add a product to the fabric membership list through the Fabric Binding option (SANtegrity Binding feature), but an entry already exists in the with the same WWN.	Enter a unique WWN for the Director or Edge Switch at the **Add Detached Switch** dialog box.
Too many members defined.	The maximum number of zone members that can be defined was reached.	Delete an existing zone member before adding a new zone member.
You do not have a compatible version of the HAFM appliance software. In order for the HAFM application to function properly, a compatible version must be installed on the client machine. Click **OK** to install a compatible version.	The *HAFM* application version running on the HAFM appliance differs from the version running on the remote workstation (client). A compatible version must be downloaded from the HAFM appliance.	Download a compatible version of the *HAFM* application to the remote workstation (client) using the Web install procedure.
You do not have rights to perform this action.	Configured user rights do not allow this operation to be performed.	Verify user rights with the customer's network administrator and change as required.
You must define an SMTP server address.	A simple mail transfer protocol (SMTP) server address must be defined and configured for e-mail to be activated.	Define the SMTP server address at the **Configure E-Mail** dialog box.

Table 24: HAFM application messages (Continued)

Message	Description	Action
You must define at least one E-mail address.	At least one e-mail address must be defined and configured for e-mail to be activated.	Define an e-mail address at the **Configure E-Mail** dialog box.
You must define at least one remote network address.	At least one IP address for a remote workstation must be configured for a remote session to be activated.	Define an IP address for at least one remote workstation at the **Session Options** dialog box.
You must download the HAFM client via the web install.	An attempt was made to download the *HAFM* application to a remote workstation (client) using an improper procedure.	Download a compatible version of the *HAFM* application to the remote workstation (client) using the Web install procedure.
Zones configured with port numbers are ignored in Open Fabric Mode.	While in Open Fabric mode, zones configured using port numbers are enforced through world-wide names.	Informational message only–no action is required.
Zones must be defined before creating a zone set.	You cannot create a zone set without any zones defined for the HAFM.	Define zones using the **New Zone** dialog box.
Zoning by port number is not supported in Open Fabric Mode.	You cannot specify an item for zoning by port number if the *HAFM* application is set to Open Fabric Mode.	Either define zones by device WWN or change to Homogeneous Fabric 1.0 mode in the **Configure Operation Mode** dialog box of the *Element Manager* application.
Zoning name already exists.	Duplicate zone names are not allowed in the zoning library.	Modify (to make it unique) or delete the duplicate zone name.

Element Manager Messages

This section lists Edge Switch 2/32 *Element Manager* application information and error messages in alphabetical order.

Table 25: Edge Switch 2/32 **Element Manager Messages**

Message	Description	Action
Activating this configuration will overwrite the current configuration.	Confirmation to activate a new address configuration.	Click **Yes** to confirm activating the new address configuration or **No** to cancel the operation.
All configuration names must be unique.	All address configurations must be saved with unique names.	Save the configuration with a different name that is unique to all saved configurations.
All port names must be unique.	A duplicate port name was entered. Every configured port name must be unique.	Reconfigure the port with a unique name.
Another Element Manager is currently performing a firmware install.	Only one firmware install to a specific switch can take place at a time.	Wait for the current firmware install to complete and try again.
Are you sure you want to delete firmware version?	Requesting confirmation to delete the firmware version. Firmware library can hold only eight firmware versions.	Click **Yes** to confirm the firmware deletion or **No** to cancel the operation.
Are you sure you want to delete this address configuration?	Confirmation to delete the selected address configuration.	Click **Yes** to confirm the deletion of the address configuration or **No** to cancel the operation.
Are you sure you want to send firmware version?	Confirmation to send a firmware version to the switch.	Click **Yes** to confirm sending the firmware version to the switch, or no to cancel the operation.

Table 25: Edge Switch 2/32 **Element Manager Messages (Continued)**

Message	Description	Action
Cannot change Port Type while Management Style is FICON without SANtegrity feature. Please contact your sales representative.	Firmware is below the required level and you attempted to change a port type in the Configure Ports dialog box while **FICON** management style, but the optional SANtegrity Binding feature is not installed.	Informational message. If the firmware is below the required level, install SANtegrity Binding before changing port types in the Configure Ports dialog box while in **FICON** management style.
Cannot disable Switch Binding while Enterprise Fabric Mode is active and the switch is Online.	User attempted to disable switch binding through the **Switch Binding Change State** dialog box, but Enterprise Fabric Mode is enabled.	You must either disable Enterprise Fabric Mode using the **Enterprise Fabric Mode** dialog box in the *HAFM* application or set the switch offline before you can disable Switch Binding.
Cannot disable Insistent Domain ID while Fabric Binding is active.	User attempted to disable the Insistent Domain ID parameter through the **Configure Switch Parameters** dialog box, but Fabric Binding is enabled.	Disable Fabric Binding through the **Fabric Binding** dialog box before disabling these parameters.
Cannot enable beaconing on a failed FRU.	Occurs when selecting Enable Beaconing option for a failed FRU.	Replace FRU and enable beaconing again or enable beaconing on operating FRU.
Cannot enable beaconing while the system error light is on.	Beaconing cannot be enabled while the system error light is on.	Select **Clear System Error Light** from **Product** menu to clear error light, then enable beaconing.

Table 25: Edge Switch 2/32 **Element Manager Messages (Continued)**

Message	Description	Action
Cannot enable Open Trunking while Enterprise Fabric Mode is active and the switch is online.	Enterprise Fabric mode is active and the switch is online and user is attempting to enable Open Trunking. This message only displays if the optional Open Trunking feature is installed.	Perform either of the following steps: ■ Disable Enterprise Fabric Mode option by selecting the appropriate fabric in the Fabric Tree portion of the HAFM window (**Fabrics** tab) and then selecting **Enterprise Fabric Mode** from the **Fabrics** menu. When the **Enterprise Fabric Mode** dialog box displays, click **Start** and follow prompts to disable the feature. ■ Set the switch offline through the **Set Online State** dialog box. Display this dialog box by selecting **Set Online State** from the Element Manager **Maintenance** menu.
Cannot have E-Ports if Management Style is FICON unless SANtegrity feature is installed. Please contact your sales representative.	Firmware is below the required level and you attempted to change management style from **Open Systems** to **FICON** management style with E_Ports configured, but SANtegrity Binding is not installed.	Informational message. If firmware is below the required level and you install SANtegrity Binding before changing to **FICON** management style, then E_Ports will remain as E_Ports when you change to **FICON** management style. If SANtegrity Binding is not installed, setting a switch to **FICON** management style will change all E_ports to G_Ports.
Cannot have spaces in field.	Spaces are not allowed in this field.	Remove the spaces or retype the field without spaces.

Table 25: Edge Switch 2/32 **Element Manager Messages (Continued)**

Message	Description	Action
Cannot install firmware to a switch with a failed CTP card.	Firmware cannot be installed on a switch with a defective CTP card.	Note that the CTP card is not a FRU. If it fails, the switch must be replaced. After replacement, retry the firmware install to the switch.
Cannot perform this operation while the switch is offline.	This operation cannot take place while the switch is offline.	Configure the switch offline through the **Set Online State** dialog box then retry the operation.
Cannot retrieve current SNMP configuration.	The current SNMP configuration cannot be retrieved. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot retrieve diagnostics results.	Diagnostics results cannot be retrieved. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot retrieve information for port.	Information for the port cannot be retrieved. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot retrieve port configuration.	Port configuration cannot be retrieved. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot retrieve port information.	Port information cannot be retrieved. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot retrieve port statistics.	Port statistics cannot be retrieved. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot retrieve switch date and time.	Switch date and time cannot be retrieved. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot retrieve switch state.	Switch state cannot be retrieved. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot run diagnostics on a port that is failed.	Port diagnostics cannot be performed on a port that has failed.	Run diagnostics only on an operational port.

Table 25: Edge Switch 2/32 **Element Manager Messages (Continued)**

Message	Description	Action
Cannot run diagnostics on an active E-port.	Port diagnostics cannot be performed on an active E-port.	Run diagnostics on an E-port only when it is not active.
Cannot run diagnostics while a device is logged-in to the port.	A device is logged in to the port where a diagnostic test is attempted.	Log out the device and run the diagnostic test again.
Cannot run diagnostics. The port is not installed.	Port diagnostics cannot be performed when the port is not installed.	Run diagnostics only on a port that is installed.
Cannot save port configuration.	Port configuration cannot be saved. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot save SNMP configuration.	SNMP configuration cannot be saved. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot set all ports to 1 Gb/sec due to port speed restriction on some ports.	Displays if you try to set ports to operate at 1 Gb/sec data speed through the **Configure Ports** dialog box and some ports do not support speed configuration.	Replace ports that do not support speed configuration with those that do support more than one speed configuration.
Cannot set all ports to 2Gb/sec due to port speed restriction on some ports.	Displays if you try to set ports to operate at 2 Gb/sec data speed through the **Configure Ports** dialog box and some ports do not support speed configuration.	Replace ports that do not support speed configuration with those that do support more than one speed configuration.
Cannot set all ports to Negotiate due to port speed restriction on some ports.	Displays if you try to set all ports to Negotiate through the **Configure Ports** dialog box and some ports do not support speed configuration.	Replace ports that do not support speed configuration with those that do support more than one speed configuration.

Table 25: Edge Switch 2/32 **Element Manager Messages (Continued)**

Message	Description	Action
Cannot set Fibre Channel parameters.	Fibre Channel parameters cannot be set. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot set switch date and time.	Switch date and time cannot be set. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot set switch state.	Switch state cannot be set. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot set write authorization without defining a community name.	A community name was not defined in the **Configure SNMP** dialog box for the write authorization selected.	Provide a name in the name field where write authorization is checked.
Cannot start data collection.	Data collection cannot be started. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot start firmware install while CTP synchronization is in progress.	CTP synchronization is in progress while you are attempting to install firmware.	Wait for the CTP synchronization to complete before starting the firmware install.
Cannot start port diagnostics.	Port diagnostics cannot be started. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Cannot swap an uninstalled port.	A port swap cannot be performed when the port is not installed.	Perform a swap only on a port that is installed.
Click OK to remove all contents from log.	Requesting confirmation that you want all contents removed from the log.	Click **OK** to continue or **Cancel** to cancel the operation.
Continuing may overwrite host programming. Continue?	Configurations sent from the host may be overwritten by HAFM.	Continuing will activate the current configuration, which may have been configured by a FICON host.

Table 25: Edge Switch 2/32 **Element Manager Messages (Continued)**

Message	Description	Action
Could not export log to file.	A file I/O error occurred. The log file could not be saved to the specified destination.	Ensure file name and drive are correct.
Could not find firmware file.	Firmware file selected was not found in the FTP directory.	Ensure file name and directory are correct.
Could not find firmware file.	The selected file is not a firmware file.	Obtain a valid firmware file from your service representative.
Could not remove dump files from server.	Dump files could not be removed from server. Link may be down or switch may be busy.	Retry the operation later. If the condition persists, contact support personnel.
Could not stop port diagnostics.	Port diagnostics could not be stopped. Link may be down or switch may be busy.	Retry the operation later. If the condition persists, contact support personnel.
Could not write firmware to flash.	Firmware could not be written to flash memory.	Try again. If problem persists, contact support personnel.
CUP name and port name are identical.	Within the address configuration, one or more of the port names are the same as the CUP name.	Make sure all names are unique for the ports and CUP name.
Date entered is invalid.	Date entered incorrectly.	Verify that the number of days in the month is valid.
Device applications should be terminated before starting diagnostics. Press NEXT to continue.	Device application is not terminated.	Terminate device application before running port diagnostics.

Table 25: Edge Switch 2/32 **Element Manager Messages (Continued)**

Message	Description	Action
[device WWN] cannot be removed from the Switch Membership List while participating in Switch Binding. The device must be isolated from the switch, or Switch Binding deactivated before it can be removed.	User attempted to remove a device WWN from the Switch Membership List (SANtegrity Binding feature) while Switch Binding is enabled.	Remove the device from the switch by blocking the port, setting the switch offline, or disabling Switch Binding through the **Switch Binding Change State** dialog box before removing devices form the Switch Membership List.
Disabling Insistent Domain ID will disable Fabric Binding. Do you want to continue?	Fabric Binding is enabled through the HAFM and user attempted to disable Insistent Domain ID in the **Configure Switch Parameters** dialog box.	Click **Yes** if you want to continue and disable Fabric Binding.
Disabling Switch Binding will disable Enterprise Fabric Mode. Do you want to continue?	User attempting to disable Switch Binding through the **Switch Binding State Change** dialog box, but Enterprise Fabric Mode is enabled	Disable Enterprise Fabric Mode using the **Enterprise Fabric Mode** dialog box in the HAFM before disabling Switch Binding.
Do you want to continue with IPL?	Requesting confirmation to proceed with an IPL.	Click **Yes** to confirm the IPL or **Cancel** to cancel the operation.
Duplicate community names require identical write authorizations.	Duplicate community names exist that have conflicting or different write authorizations.	Verify community names and whether a community name is duplicated with different write authorizations.
Enterprise Fabric Mode will be disabled if any of the following parameters are disabled: Insistent Domain ID, Rerouting Delay, Domain RSCN's. Do you want to continue?	User attempted to disable these parameters in the **Configure Switch Parameters** dialog box while the Edge Switch was online, but Enterprise Fabric Mode (SANtegrity Binding feature) is enabled.	Click **Yes** if you want to continue, and disable Enterprise Fabric Mode.

Table 25: Edge Switch 2/32 **Element Manager Messages (Continued)**

Message	Description	Action
Error retrieving port information.	An error occurred while retrieving port information. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Error retrieving port statistics.	An error occurred while retrieving port statistics. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Error stopping port diagnostics.	An error occurred while attempting to stop the port diagnostics from running. The link is down or busy.	Retry the operation later. If the condition persists, contact support personnel.
Error transferring files <message>.	An error occurred while attempting to download files.	Retry the operation. If the condition persists, contact support personnel.
Feature not supported. The switch must be running version 05.00.00 or higher.	The enterprise operating system version on Edge Switch is lower than 05.00.00. This message only displays if the optional Open Trunking feature is installed.	Install operating system version 5.00.00 or higher on the hardware product.
Field cannot be blank.	A blank field is not allowed in this dialog.	Enter the required information in the blank field.
Field has exceeded maximum number of characters.	The maximum number of data entry characters allowed in the field was exceeded.	Enter the information using the prescribed number of characters.
File transfer aborted.	User has stopped the file transfer.	N/A. An informational message.
File transfer is in progress.	Firmware or data collection is being transferred.	N/A. An informational message.
Firmware download timed out.	The switch did not respond in the time allowed. The status of the firmware install operation is unknown.	Retry the operation. If the problem persists, contact support personnel.

Table 25: Edge Switch 2/32 **Element Manager Messages (Continued)**

Message	Description	Action
Firmware file I/O error.	Firmware file input/output error occurred.	Contact support personnel.
Firmware file not found.	Firmware file deleted from the HAFM appliance.	Add firmware to library.
Incompatible configuration between management style and management server.	If the Firmware is below the required level, only **FICON** management style is allowed if the FICON Management Server feature is enabled. You attempted to enable **Open Systems** management style.	Disable FICON Management Server, enable the Open Systems Management Server, or enable the **Open Systems** management style.
Incorrect product type.	When configuring a new product through the **New Product** dialog box, an incorrect product was selected for the network address.	Select the correct product type for the product with the network address.
Installing this feature key, while online, will cause an IPL operation on the switch and a momentary loss of LAN connection. This operation is non-disruptive to the Fibre Channel traffic. Do you wish to continue installing this feature key?	If the Edge Switch is online, installing the new feature key will cause an internal program load (IPL). The LAN connection to the HAFM appliance will be lost momentarily, but Fibre Channel traffic will not be affected.	Select **Yes** to install the feature key or **No** to not install.
Internal file transfer error received from switch.	Switch detected an internal file transfer error.	Contact support personnel.
Invalid character in field.	Invalid character in the input field.	Re-enter the field information.
Invalid configuration name.	Attempted to save an address configuration name with an invalid name.	Use up to 24 alphanumeric characters, including spaces, hyphens and underscores.

Table 25: Edge Switch 2/32 **Element Manager Messages (Continued)**

Message	Description	Action
Invalid feature key.	The feature key was not recognized.	Re-enter the feature key noting the key is case-sensitive and to include the dashes.
Invalid firmware file.	Selected file is not a firmware file.	Select the correct firmware file.
Invalid HAFM appliance address.	The IP address specified for the HAFM appliance is unknown to the domain name server (invalid).	Verify and enter a valid HAFM appliance IP address.
Invalid network address.	Network address specified is not known by the domain name server.	Check the input address and specify the correct network address.
Invalid port number.	Port number must be within the range of ports for the specific switch model.	Enter a port number within the correct range.
Invalid port number. Valid ports are (0–31).	Port number must be within the range of ports for the specific switch model. For this model, the valid port numbers are 0–31.	Enter a port number within the correct range.
Invalid port swap.	Port swap selection is not allowed.	Ensure that each port selected for swap has not been previously swapped.
Invalid response received from switch.	The switch returned an invalid response.	Resend the firmware. If the condition persists, contact support personnel.
Invalid serial number for this feature key.	The serial number and the feature key did not match.	Ensure that the feature key being installed is specifically for this switch serial number.
Invalid UDP port number.	UDP port number must be an integer from 1 through 65535.	Enter a port number from 1 through 65535.

Table 25: Edge Switch 2/32 **Element Manager Messages (Continued)**

Message	Description	Action
Invalid value for BB_Credit.	BB_Credit must be an integer from 1 through 60.	Enter a number from 1 through 60.
Invalid value for day (1–31).	Value for day must be an integer from 1 through 31.	Enter a value from 1 through 31.
Invalid value for E_D_TOV.	Value for E_D_TOV must be an integer from 2 through 600, measured in tenths of a second.	Enter a value from 2 through 600.
Invalid value for hour (0–23).	Value for hour must be an integer from 0 through 23.	Enter a value from 0 through 23.
Invalid value for minute (0–59).	Value for minute must be an integer from 0 through 59.	Enter a value from 0 through 59.
Invalid value for month (1–12).	Value for month must be an integer from 1 through 12.	Enter a value from 1 through 12.
Invalid value for R_A_TOV.	Value for R_A_TOV must be an integer from 10 through 1200. Measured in tenths of a second.	Enter a value from 10 to 1200.
Invalid value for second (0–59).	Value for second must be an integer from 0 through 59.	Enter a value from 0 through 59.
Invalid value for threshold (1-99)%.	Value entered for each port in the **Configure Open Trunking** dialog box must be in the range from 1 to 99. This message only displays if the optional Open Trunking feature is installed.	Enter a number from 1 to 99 into the **Threshold %** column of the Configure **Open Trunking** dialog box.
Invalid value for year.	Value for year must be a four-digit year after 1980.	Enter a correct four-digit value for the year.

Table 25: Edge Switch 2/32 **Element Manager Messages (Continued)**

Message	Description	Action
Invalid World Wide Name.	World Wide Name must have eight two-digit hexadecimal numbers separated by colons (xx:xx:xx:xx:xx:xx:xx:xx)	Enter a World Wide Name using eight two-digit hexadecimal numbers separated by colons in the format given in the message.
Link dropped.	Connection between HAFM appliance and the switch has been lost.	Wait for the connection to re-establish. Link re-connects are attempted every 30 seconds.
Log is currently in use.	Log is in use by another Element Manager.	Retry the operation later.
Loopback plug(s) must be installed on ports being diagnosed. Press Next to continue.	External loopback diagnostics require an optical loopback plug to be installed.	Ensure that an optical loopback plug is installed in port optical transceiver before running external wrap diagnostic testing.
Maximum number of versions already installed.	The maximum number of firmware versions has been reached.	Delete a firmware version before adding a new firmware version.
No file was selected.	Action requires you to select a file	Select a file.
No firmware version file was selected.	A file was not selected in the **Firmware Library** dialog box before an action, such as modify or send was performed.	Click a firmware version in the dialog box to select it, then perform the action again.
No firmware versions to delete.	There are no firmware versions in the firmware library to delete.	N/A. An informational message.
Non-redundant switch must be offline to install firmware.	Since the switch has only a single CTP card, it must be offline to initiate a firmware installation. Note that the CTP card is an internal component and not a FRU.	Take switch offline and try again.
Not all of the optical transceivers are installed for this range of ports.	Some ports in the specified range do not have optical transceivers installed.	Use a port range that is valid for the ports installed.

Table 25: Edge Switch 2/32 **Element Manager Messages (Continued)**

Message	Description	Action
Open Trunking is not installed for this product. Please contact your sales representative.	The Open Trunking feature key has not been enabled. This message only displays if the optional Open Trunking feature is installed.	Enter the feature key into the **Configure Feature Key** dialog box and enable the key. If you require a feature key, see your account representative.
Performing this operation will change the current state to Offline.	This operation causes the switch to go offline.	N/A. An informational message.
Performing this operation will change the current state to Online.	This operation causes the switch to go online.	N/A. An informational message.
Performing this action will overwrite the date/time on the switch.	Warning that occurs when configuring the date and time through the **Configure Date and Time** dialog box, that the new time or date will overwrite the existing time or date set for the switch.	Verify that you want to overwrite the current date or time.
Periodic Date/Time synchronization must be cleared before enabling switch clock alert.	Action cannot be performed because Periodic Date/Time Synchronization option is active.	Click **Periodic Date/Time Synchronization** check box in **Configure Date and Time** dialog box (**Configure** menu) to clear check mark and disable periodic date/time synchronization.
Port binding was removed from attached devices that are also participating in Switch Binding.	Informational message. User has removed Port Binding from attached devices, but one or more of these devices is still controlled by Fabric Binding.	Review the Switch Binding Membership List to determine if the devices should be members.
Port cannot swap to itself.	Port addresses entered in the **Swap Ports** dialog box are the same.	Make sure that address in the first and second port address fields are different.

Table 25: Edge Switch 2/32 **Element Manager Messages (Continued)**

Message	Description	Action
Port diagnostics cannot be performed on an inactive port.	This displays when port diagnostics is run on a port in an inactive state.	Run the diagnostics on an active port.
Port speeds cannot be configured at a higher rate than the director/switch speed.	This displays when you configure a port to 2 GB/sec and the switch speed is set to 1 Gb/sec.	Set the port speed to 1 Gb/sec in the **Configure Operating Parameters** dialog box.
Element Manager error <number>.	The switch Element Manager encountered an internal error and cannot continue.	Report the problem to support personnel.
Element Manager instance is currently open.	An Element Manager window is currently open.	N/A. Informational message.
R_A_TOV must be greater than E_D_TOV.	R_A_TOV must be greater than E_D_TOV.	Change one of the values so that R_A_TOV is greater than E_D_TOV.
Resource is unavailable.	The specified operation cannot be performed because the product is unavailable.	Verify that the HAFM appliance-to-product link is up. If the link is up, the HAFM appliance may be busy. Try the operation again later.
SANtegrity Feature not installed. Please contact your sales representative.	The user selected Switch Binding from the **Configure** menu, but the optional SANtegrity Binding feature is not installed.	Install the SANtegrity key through the **Configure Feature Key** dialog box before using Switch Binding features.
Send firmware failed.	Send firmware operation has failed.	Retry the operation. If the condition persists, contact support personnel.
SNMP trap address not defined.	An SNMP trap address must be defined if a community name is defined.	Define an SNMP address.

Table 25: Edge Switch 2/32 **Element Manager Messages (Continued)**

Message	Description	Action
Stop diagnostics failed. The test is already running.	Diagnostics for the port was not running and the Stop was selected on the **Port Diagnostics** dialog box. Diagnostics quit for the port for some reason, but the **Stop** button remains enabled.	Verify port operation. Retry diagnostics for port and select **Stop** from the dialog box. If problem persists, contact your service representative.
Stop diagnostics failed. The test was not running.	The action to stop diagnostics failed because the test was not running.	N/A. Informational message.
Switch Binding was removed from attached devices that are also participating in Port Binding. Please review the Port Binding Configuration.	The device WWNs were removed from the Switch Membership List (SANtegrity Binding feature), but you should note that one or more of these devices still has security control in port binding.	Verify that the security level for each device is as required by reviewing the Bound WWN list in the **Configure Ports** dialog box.
System diagnostics cannot run. The Operational Status is invalid.	System diagnostics cannot run on switches with failed ports.	Replace failed ports.
The add firmware process has been aborted.	User has ended the add firmware process.	N/A. An informational message.
The data collection process failed.	An error occurred in the data collection process.	Contact support personnel.
The data collection process has been aborted.	User has ended the data collection process.	N/A. An informational message.
The default zone must be disabled to configure.	The message displays when the user attempts to change the interoperability mode to open fabric and the default zone is enabled	Disable the default zone and repeat the operation.

Table 25: Edge Switch 2/32 **Element Manager Messages (Continued)**

Message	Description	Action
The switch is busy saving maintenance information.	The switch is busy with a maintenance operation.	Retry the operation later. If the condition persists, contact support personnel.
The following parameters cannot be disabled while Enterprise Fabric Mode is active: Insistent Domain ID, Rerouting Delay, Domain RSCN's.	User attempted to disable these parameters in the **Configure Switch Parameters** dialog box while Enterprise Fabric Mode is enabled.	Disable Enterprise Fabric Mode through the **Enterprise Fabric Mode** dialog box in the HAFM, then disable the parameters.
The firmware file is corrupted.	A firmware file has corrupt data.	Contact support personnel.
The firmware version already exists.	Firmware version already exists in the database.	N/A. An informational message.
The HAFM appliance is busy processing a request from another Element Manager	The HAFM appliance could not process the current request because it is busy handling a request from another Element Manager.	Retry the operation later. If the condition persists, contact support personnel.
The link to the switch is not available.	The link from the HAFM appliance to the switch is not available.	Check Ethernet connection.
The maximum number of address configurations has been reached.	The maximum number of saved address configurations has been reached.	Delete configurations no longer needed to allow new configuration to be saved.
The optical transceiver is not installed.	No information available for a port that is not installed.	Ensure the optical transceiver is installed and fully seated.
The switch did not respond in the time allowed.	A time out was reached waiting for the switch to respond to the action.	Try action again.
The IPL configuration cannot be deleted.	Deletion of the IPL address configuration was attempted and was not allowed.	Cancel the operation.

Table 25: Edge Switch 2/32 **Element Manager Messages (Continued)**

Message	Description	Action
This feature has not been installed. Please contact your sales representative.	Indicator that the feature has not been installed on this switch.	Contact your sales representative to obtain the desired feature.
This feature key does not include all of the features currently installed and cannot be activated while the switch is online.	The feature set currently installed for this system contains features that are not being installed with the new feature key. To activate the new feature key, you must set the Edge Switch offline. Activating the new feature set, however, will remove current features not in the new feature set.	Set the Edge Switch offline through the **Set Online State** dialog box, then activate the new feature key using the **Configure Feature Key** dialog box.
This feature key does not include all of the features currently installed. Do you want to continue with feature key activation?	The feature set currently installed for this system contains features that are not being installed with the new feature key.	Click **Yes** to activate the feature key and remove current features not in the new feature set or **No** to cancel.
Threshold alerts are not supported on firmware earlier than 01.03.00.	Threshold alerts are not supported in firmware releases before 1.03.00.	N/A. Informational message.
Unable to change to incompatible firmware release.	The user tried to download a firmware release that is not compatible with the current product configuration.	Refer to the release notes or contact customer support.
Unable to save data collection file to destination.	Could not save data collection file to the specified drive (hard drive, network).	Retry the operation. If the condition persists, contact support personnel.
You do not have rights to perform this action.	User does not have the rights to perform this action.	N/A. Informational message.

Event Codes

B

This appendix lists all three-digit HP StorageWorks Edge Switch 2/32 event codes and provides detailed information about each code. Event codes are listed in numerical order and in tabular format.

An event is an occurrence (state change, problem detection, or problem correction) that requires user attention or that should be reported to a system administrator or service representative. An event usually indicates a switch operational state transition, but may also indicate an impending state change (threshold violation). An event may also provide information only, and not indicate an operational state change. Event codes are grouped as follows:

Events can be recorded in the switch **Event Logs** at the HAFM appliance, at a remote workstation if E-mail and call-home features are enabled, or at a simple network management protocol (SNMP) workstation. An event may also illuminate the system error (**ERR**) light-emitting diode (LED) on the front panel.

In addition to numerical event codes, the tables in this appendix also provide the following information about each code:

- **Message–**a brief text string that describes the event.
- **Severity–**a severity level that indicates event criticality as follows:
  - **0–**informational.
  - **2–**minor.
  - **3–**major.
  - **4–**severe (not operational).
- **Explanation–**a complete explanation of what caused the event.
- **Action–**the recommended course of action (if any) to resolve the problem.
- **Event Data–**supplementary event data (if any) that displays in the Event Log in hexadecimal format.
- **Distribution–**check marks in associated fields indicate where the event code is reported (front panel, HAFM appliance, or host).

System Events (000 through 199)

Table 26: Event Code 001

Message:	System power-down.						
Severity:	Informational.						
Explanation:	The switch was powered off or disconnected from the facility AC power source. The event code is distributed the next time the switch powers on, but the date and time of the code reflect the power-off time.						
Action:	No action required.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Table 27: Event Code 011

Message:	Login Server database invalid.						
Severity:	Minor.						
Explanation:	Following an initial machine load (IML) or firmware download, the Login Server database failed its cyclic redundancy check (CRC) validation. All Fabric Services databases are initialized to an empty state, resulting in an implicit Fabric logout of all attached devices.						
Action:	Perform the data collection procedure and return the backup disk to Hewlett-Packard support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔		

Table 28: Event Code 021

Message:	Name Server database invalid.						
Severity:	Minor.						
Explanation:	Following an IML or firmware download, the Name Server database failed its CRC validation. All Fabric Services databases are initialized to an empty state, resulting in an implicit Fabric logout of all attached devices.						
Action:	Perform the data collection procedure and return the backup disk to Hewlett-Packard support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔		

Table 29: Event Code 031

Message:	SNMP request received from unauthorized community.						
Severity:	Informational.						
Explanation:	An SNMP request containing an unauthorized community name was received and rejected with an error. Only requests containing authorized SNMP community names as configured through the switch *Element Manager* application are allowed.						
Action:	Add the community name to the SNMP configuration using the switch *Element Manager* application.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Table 30: Event Code 051

Message:	Management Server database invalid.						
Severity:	Minor.						
Explanation:	Following an IML, or firmware download, the Management Server database failed its CRC validation. All Management Services databases are initialized to an empty state, resulting in an implicit logout of all devices logged in to the Management Server.						
Action:	Perform the data collection procedure and return the backup disk to Hewlett-Packard support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔		

Table 31: Event Code 052

<table>
<tr><td>Message:</td><td colspan="7">Management Server internal error, asynchronous status report activation, or mode register update occurred.</td></tr>
<tr><td>Severity:</td><td colspan="7">Informational.</td></tr>
<tr><td>Explanation:</td><td colspan="7">An internal operating error was detected by the Management Server subsystem, an asynchronous status was reported to an attached host, or a mode register update occurred.</td></tr>
<tr><td>Action:</td><td colspan="7">Management Server internal error: Perform the data collection procedure and return the backup disk to Hewlett-Packard support personnel.
Asynchronous status report activation: No action required.
Mode register update: No action required.</td></tr>
<tr><td>Event Data:</td><td colspan="7">Supplementary data consists of reporting tasks of type eMST_SB2, with component_id eMSCID_SB2_CHPGM. For each type of error or indication, the subcomponent_id is:
Management Server internal error: subcomponent_id is eMS_ELR_SB2_DEVICE_PROTOCOL_ERROR or eMS_ELR_SB2_MSG_PROCESSING_ERROR.
Asynchronous status report activation: subcomponent_id is eSB2_CP_RER_ASYNCH_STATUS_REPORTING.
Mode register update: subcomponent_id is eMS_ELR_MODE_REGISTER_UPDATE.</td></tr>
<tr><td rowspan="3">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Appliance</td><td colspan="2">Host</td></tr>
<tr><td>EWS Event Log</td><td>System Error LED</td><td>Event Log</td><td>E-Mail</td><td>Call Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td>✔</td><td></td><td>✔</td><td></td><td></td><td>✔</td><td></td></tr>
</table>

Table 32: Event Code 061

Message:	Fabric Controller database invalid.						
Severity:	Minor.						
Explanation:	Following an IML, or firmware download, the Fabric Controller database failed its CRC validation. All Fabric Controller databases are initialized to an empty state, resulting in a momentary loss of interswitch communication capability.						
Action:	Perform the data collection procedure and return the backup disk to Hewlett-Packard support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔		

Table 33: Event Code 062

Message:	Maximum interswitch hop count exceeded.						
Severity:	Informational.						
Explanation:	The fabric controller software detected that a path to another fabric element (Director or Edge Switch) traverses more than seven interswitch links (ISLs or hops). This may result in Fibre Channel frames persisting in the fabric longer than standard timeout values allow.						
Action:	If possible, reconfigure the fabric so the path between any two Directors or Edge Switches traverses no more than seven ISLs.						
Event Data:	Byte **0** = domain ID of the fabric element (Director or Edge Switch) more than seven hops away.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Table 34: Event Code 063

Message:	Remote switch has too many ISLs.						
Severity:	Major.						
Explanation:	The switch indicated in the event data (Domain ID) has too many ISLs attached to it. That switch is unreachable from this switch.						
Action:	Reduce the ISLs on the indicated fabric element to a number within the limits specified.						
Event Data:	Byte **0** = domain ID of the fabric element (director or switch) with too many ISLs.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Table 35: Event Code 070

Message:	E_Port is segmented.
Severity:	Informational.
Explanation:	A switch E_Port recognized an incompatibility with an attached fabric element (Director or Edge Switch), preventing the switch from participating in the fabric. A segmented port does not transmit Class 2 or Class 3 traffic (data from attached devices), but transmits Class F traffic (management and control data from the attached Director or Edge Switch). Refer to the event data for the segmentation reason.
Action:	Action depends on the segmentation reason specified in the event data.

Table 35: Event Code 070 (Continued)

Event Data:	The first byte of event data (byte **0**) specifies the E_Port number. The fifth byte (byte **4**) specifies the segmentation reason as follows: **1 = Incompatible operating parameters.** Ether the resource allocation time out value (R_A_TOV) or error detect time out value (E_D_TOV) is inconsistent between the switch and another fabric element (Director or Edge Switch). Modify the R_A_TOV and E_D_TOV to make the values consistent for all fabric Directors and Edge Switches. **2 = Duplicate domain ID.** The switch has the same preferred domain ID as another fabric element (Director or Edge Switch). Modify the switch Domain ID to make it unique. **3 = Incompatible zoning configurations.** The same name is applied to a zone for the switch and another fabric element (Director or Edge Switch), but the zones contain different zone members. Modify the zone name to make it unique, or ensure zones with the same name contain identical zone members. **4 = Build fabric protocol error.** A protocol error was detected during incorporation of the switch into the fabric. Disconnect the E_Port link, reconnect the link, and initial program load (IPL) the switch. If the condition persists, perform the data collection procedure and return the backup disk to Hewlett-Packard support personnel. **5 = No principal switch.** No Director or Edge Switch in the fabric can become the principal switch. Modify the switch priority to any value other than 255. **6 = No response from attached switch (hello timeout).** The switch periodically verifies operation of attached fabric elements (Director or Edge Switch). The switch E_Port (at the operational switch) times out and segments if the attached device does not respond. Check the status of the attached Director or Edge Switch. If the condition persists, perform the data collection procedure (at the attached device) and return the backup disk to Hewlett-Packard support personnel.

Table 35: Event Code 070 (Continued)

Event Code: 070 (continued)							
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Table 36: Event Code 071

Message:	Switch is isolated.
Severity:	Informational.
Explanation:	The switch is isolated from other fabric elements (Director or Edge Switch). This event code is accompanied by one or more **070** event codes. Refer to the event data for the segmentation reason.
Action:	Action depends on the segmentation reason specified in the event data.
Event Data:	The first byte of event data (byte **0**) specifies the E_Port number. The fifth byte (byte **4**) specifies the segmentation reason as follows: **1 = Incompatible operating parameters.** Ether the resource allocation time out value (R_A_TOV) or error detect time out value (E_D_TOV) is inconsistent between the switch and another fabric element (Director or Edge Switch). Modify the R_A_TOV and E_D_TOV to make the values consistent for all fabric Directors and Edge Switches. **2 = Duplicate domain ID.** The switch has the same preferred domain ID as another fabric element (Director or Edge Switch). Modify the switch's Domain ID to make it unique. **3 = Incompatible zoning configurations.** The same name is applied to a zone for the switch and another fabric element (Director or Edge Switch), but the zones contain different zone members. Modify the zone name to make it unique, or ensure zones with the same name contain identical zone members.

Table 36: Event Code 071 (Continued)

<table>
<tr><td></td><td colspan="7"></td></tr>
<tr><td>Event Data (continued):</td><td colspan="7">4 = Build fabric protocol error. A protocol error was detected during incorporation of the switch into the fabric. Disconnect the E_Port link, reconnect the link, and IPL the switch. If the condition persists, perform the data collection procedure and return the backup disk to Hewlett-Packard support personnel.
5 = No principal switch. No Director or Edge Switch in the fabric can become the principal switch. Modify the switch priority to any value other than 255.
6 = No response from attached switch (hello timeout). The switch periodically verifies operation of attached fabric elements (Director or Edge Switch). The switch E_Port (at the operational switch) times out and segments if the attached device does not respond. Check the status of the attached Director or Edge Switch. If the condition persists, perform the data collection procedure (at the attached device) and return the backup disk to Hewlett-Packard support personnel.</td></tr>
<tr><td rowspan="2">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Appliance</td><td colspan="2">Host</td></tr>
<tr><td>EWS Event Log</td><td>System Error LED</td><td>Event Log</td><td>E-Mail</td><td>Call Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td></td><td>✔</td><td></td><td>✔</td><td></td><td></td><td></td><td></td></tr>
</table>

Table 37: Event Code 072

<table>
<tr><td>Message:</td><td colspan="7">E_Port connected to unsupported switch.</td></tr>
<tr><td>Severity:</td><td colspan="7">Informational.</td></tr>
<tr><td>Explanation:</td><td colspan="7">The switch is attached (through an ISL) to an incompatible fabric element (Director or Edge Switch).</td></tr>
<tr><td>Action:</td><td colspan="7">Disconnect the ISL.</td></tr>
<tr><td>Event Data:</td><td colspan="7">No supplementary data included with this event.</td></tr>
<tr><td rowspan="2">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Appliance</td><td colspan="2">Host</td></tr>
<tr><td>EWS Event Log</td><td>System Error LED</td><td>Event Log</td><td>E-Mail</td><td>Call Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td></td><td>✔</td><td></td><td>✔</td><td></td><td></td><td></td><td></td></tr>
</table>

Table 38: Event Code 073

Message:	Fabric initialization error.						
Severity:	Informational.						
Explanation:	An error was detected during the fabric initialization sequence, most likely caused by frame delivery errors. Event data is intended for engineering evaluation.						
Action:	Perform the data collection procedure and return the backup disk to Hewlett-Packard support personnel.						
Event Data:	Byte **0** = error reason code for engineering evaluation. Bytes **4**–**9** = port numbers for which problems were detected.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Table 39: Event Code 074

Message:	ILS frame delivery error threshold exceeded.						
Severity:	Informational.						
Explanation:	Fabric controller frame delivery errors exceeded an E_Port threshold and caused fabric initialization problems (**073** event code). Most fabric initialization problems are caused by control frame delivery errors, as indicated by this code. Event data is intended for engineering evaluation.						
Action:	Perform the data collection procedure and return the backup disk to Hewlett-Packard support personnel.						
Event Data:	Byte **0** = E_Port number reporting the problem. Byte **4**–**8** = Count of frame delivery timeouts. Byte **9**–**11** = Count of frame delivery aborts.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Table 40: Event Code 080

Message:	Unauthorized world-wide name.						
Severity:	Informational.						
Explanation:	The world-wide name of the device or switch plugged in the indicated port is not authorized for that port.						
Action:	Change the port binding definition or plug the correct device or switch into this port.						
Event Data:	Byte **0** = Port number reporting the unauthorized connection. Bytes **1**–**3** = reserved. Bytes **4**–**11** = WWN of the unauthorized device or fabric element.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔	✔		✔	

Table 41: Event Code 081

Message:	Invalid attachment.
Severity:	Informational.
Explanation:	A switch port recognized an incompatibility with the attached fabric element or device and isolated the port. An isolated port does not transmit Class 2, Class 3, or Class F traffic. Refer to the event data for the reason.
Action:	Action depends on the reason specified in the event data.

Table 41: Event Code 081 (Continued)

Event Data:	The first byte of event data (byte **0**) specifies the port number. The fifth byte (byte **4**) specifies the isolation reason as follows: **1 = Unknown**–Isolation reason is unknown, but probably caused by failure of a device attached to the switch through an E_Port connection. Fault isolate the failed device or contact support personnel to report the problem. **2 = ISL connection not allowed**–The port connection conflicts with the configured port type. Change the port type to F_Port if the port is cabled to a device, or E_Port if the port is cabled to a fabric element to form an ISL. **3 = Incompatible switch**–The switch returned a `Process ELP Reject-Unable to Process` reason code because the attached fabric element is not compatible. Set the switch operating mode to Homogeneous Fabric 1.0 if connected to an HP product. Set the switch operating mode to Open Fabric 1.0 if connected to an open-fabric compliant product manufactured by a different vendor. **4 = Incompatible switch**–The switch returned a *Process* `ELP Reject-Invalid Revision Level` reason code because the attached fabric element is not compatible. Set the switch operating mode to Homogeneous Fabric 1.0 if connected to an HP product. Set the switch operating mode to Open Fabric 1.0 if connected to an open-fabric compliant product manufactured by a different vendor. **5 = Loopback plug connected**–A loopback plug is connected to the port with no diagnostic test running. Remove the loopback plug. **6 = N_Port connection not allowed**–The switch is connected to a fabric element through a port configured as an F_Port. Change the port type to E_Port. **7 = Non-HP switch at other end**–The attached fabric element is not an HP product. Set the switch operating mode to Open Fabric 1.0 if connected to an open-fabric compliant product manufactured by a different vendor. **A = Unauthorized port binding WWN**–The device WWN or nickname used to configure port binding for this port is not valid. Reconfigure the port with the WWN or nickname authorized for the attached device.

Table 41: Event Code 081 (Continued)

<table>
<tr><td></td><td colspan="7">B = Unresponsive node–The attached node did not respond, resulting in a G_Port ELP timeout. Check the status of the attached device and clean the link's fiber-optic components (cable and connectors). If the problem persists, contact support personnel to report the problem.

C = ESA security mismatch–Processing of the Exchange Security Attribute (ESA) frame detected a security feature mismatch. The fabric binding and switch binding parameters for this switch and the attached fabric element must agree. At the Fabric Binding and Switch Binding–State Change dialog boxes, ensure the parameters for both fabric elements are compatible, or disable the fabric and switch binding features.

D = Fabric binding mismatch–Fabric binding is enabled and an attached fabric element has an incompatible fabric membership list. At the Fabric Binding dialog box, update the fabric membership list for both fabric elements to ensure compatibility, or disable the fabric binding feature.

E = Authorization failure reject–The fabric element connected to the switch through an ISL detected a security violation. As a result, the switch received a generic reason code and set the port to an invalid attachment state. Check the port status of the attached fabric element and clean the link's fiber-optic components (cable and connectors). If the problem persists, contact support personnel to report the problem.

F = Unauthorized switch binding WWN–Switch binding is enabled and an attached device or fabric element has an incompatible switch membership list. At the Switch Binding–Membership List dialog box, update the switch membership list for the switch and the attached device or fabric element to ensure compatibility, or disable the switch binding feature.

11 = Fabric mode mismatch–Based on the ELP revision level, a connection was not allowed because an HP switch in legacy mode is attached to an HP switch in Open Fabric mode, or an HP switch in Open Fabric mode is attached to an OEM switch at an incorrect ELP revision level. Update the fabric mode for one switch using the Interop Mode drop-down list at the Configure Fabric Parameters dialog box.

12 = CNT WAN extension mode mismatch–Based on switch-to-switch differences between the ELP maximum frame sizes allowed, a connection was not allowed to a switch set to Computer Network Technologies (CNT) wide area network (WAN) extension mode. Contact Computer Network Technologies for support.</td></tr>
<tr><td rowspan="3">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Appliance</td><td colspan="2">Host</td></tr>
<tr><td>EWS Event Log</td><td>System Error LED</td><td>Event Log</td><td>E-Mail</td><td>Call Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td>✔</td><td></td><td>✔</td><td></td><td></td><td></td><td></td></tr>
</table>

Table 42: Event Code 120

Message:	Error detected while processing system management command.						
Severity:	Informational.						
Explanation:	This event occurs when the switch receives an HAFM command that violates specified boundary conditions, typically as a result of a network error. The switch rejects the command, drops the switch-to-HAFM appliance Ethernet link, and forces error recovery processing. When the link recovers, the command can be retried.						
Action:	No action is required for an isolated event. If this event persists, perform a data collection for this switch using the *HAFM* application. Perform the data collection procedure and return the backup disk to Hewlett-Packard support personnel.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Table 43: Event Code 121

Message:	Zone set activation failed–zone set too large.						
Severity:	Informational.						
Explanation:	This event occurs when the switch receives a zone set activation command that exceeds the size supported by the switch. The switch rejects the command, drops the switch-to-HAFM appliance Ethernet link, and forces error recovery processing. When the link recovers, the command can be modified and retried.						
Action:	Reduce the size of the zone set to conform to the limit specified, then retry the activation command.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Table 44: Event Code 140

Message:	Congestion detected on an ISL.						
Severity:	Informational.						
Explanation:	Open Trunking firmware detected an ISL with Fibre Channel traffic that exceeded the configured congestion threshold.						
Action:	No action is required for an isolated event. If this event persists, relieve the congestion by adding parallel ISLs, increasing the ISL link speed, or moving device connections to a less-congested region of the fabric.						
Event Data:	Byte 0 = Port number reporting congestion.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔		✔				

Table 45: Event Code 141

Message:	Congestion relieved on an ISL.						
Severity:	Informational.						
Explanation:	Open Trunking firmware detected an ISL with Fibre Channel traffic that previously exceeded the configured congestion threshold. The congestion is now relieved.						
Action:	No action required.						
Event Data:	Byte 0 = Port number reporting congestion relieved.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔		✔				

Table 46: Event Code 142

Message:	Low BB_Credit detected on an ISL.						
Severity:	Informational.						
Explanation:	Open Trunking firmware detected an ISL with no transmission BB_Credit for a period of time that exceeded the configured low BB_Credit threshold. This indicates downstream fabric congestion.						
Action:	No action is required for an isolated event or if the reporting ISL approaches 100% throughput. If this event persists, relieve the low BB_Credit condition by adding parallel ISLs, increasing the ISL link speed, or moving device connections to a less-congested region of the fabric.						
Event Data:	Byte 0 = Port number reporting low BB_Credit.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔		✔				

Table 47: Event Code:143

Message:	Low BB_Credit relieved on an ISL.						
Severity:	Informational.						
Explanation:	Open Trunking firmware detected an ISL with no transmission BB_Credit for a period of time that previously exceeded the configured low BB_Credit threshold. The low-credit condition is now relieved.						
Action:	No action required.						
Event Data:	Byte 0 = Port number reporting low BB_Credit relieved.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔		✔				

Table 48: Event Code 150

Message:	Zone merge failure.
Severity:	Informational.
Explanation:	During ISL initialization, the zone merge process failed. Either an incompatible zone set was detected or a problem occurred during delivery of a zone merge frame. This event code always precedes a 070 ISL segmentation event code, and represents the reply of an adjacent fabric element in response to a zone merge frame. Refer to the event data for the failure reason.
Action:	Action depends on the failure reason specified in the event data.
Event Data:	Bytes 0–3 of the event data specify affected E_Port number(s). Bytes 8–11 specify the failure reason as follows: 01 = Invalid data length–An invalid data length condition caused an error in a zone merge frame. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform the data collection procedure and return the backup disk to HP support personnel. 08 = Invalid zone set format–An invalid zone set format caused an error in a zone merge frame. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform the data collection procedure and return the backup disk to HP support personnel. 09 = Invalid data–Invalid data caused a zone merge failure. Inspect bytes 12–15 of the event data for error codes. Refer to error code definitions listed on the following page to correct the problem. 0A = Cannot merge–A *Cannot Merge* condition caused a zone merge failure. Inspect bytes 12–15 of the event data for error codes. Refer to error code definitions listed on the following page to correct the problem. F0 = Retry limit reached–A retry limit reached condition caused an error in a zone merge frame. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform the data collection procedure and return the backup disk to HP support personnel. F1 = Invalid response length–An invalid response length condition caused an error in a zone merge frame. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform the data collection procedure and return the backup disk to HP support personnel. F2 = Invalid response code–An invalid response code caused an error in a zone merge frame. Disconnect the E_Port link, then reconnect the link. If the condition persists, perform the data collection procedure and return the backup disk to HP support personnel.

Table 48: Event Code 150 (Continued)

<table>
<tr><td colspan="8">Event Code: 150 (continued)</td></tr>
<tr><td>Event Data (continued):</td><td colspan="7">Bytes 12–15 of the event data specify error codes as follows:
01 = Completion fail.
03 = Zone merge error–too many zones.
04 = Zone merge error–incompatible zones.
05 = Zone merge error–too long if reason = 0A.
06 = Zone set definition too long.
07 = Zone set name too short or not authorized.
08 = Invalid number of zones.
09 = Zone merge error–default zone states incompatible if reason = 0A.
0A = Invalid protocol.
0B = Invalid number of zone members.
0C = Invalid flags.
0D = Invalid zone member information length.
0E = Invalid zone member information format.
0F = Invalid zone member information port.
10 = Invalid zone set name length.
11 = Invalid zone name length.
37 = Invalid zone name.
39 = Duplicate zone.
3C = Invalid number of zone members.
3D = Invalid zone member type.
3E = Invalid zone set name.
45 = Duplicate member in zone.
4A = Invalid number of zones.
4B = Invalid zone set size.
4D = Maximum number of unique zone members exceeded.</td></tr>
<tr><td rowspan="3">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Appliance</td><td colspan="2">Host</td></tr>
<tr><td>EWS Event Log</td><td>System Error LED</td><td>Event Log</td><td>E-Mail</td><td>Call-Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td>✔</td><td>✔</td><td>✔</td><td></td><td></td><td></td><td></td></tr>
</table>

Table 49: Event Code 151

<table>
<tr><td>Message:</td><td colspan="7">Fabric configuration failure.</td></tr>
<tr><td>Severity:</td><td colspan="7">Informational.</td></tr>
<tr><td>Explanation:</td><td colspan="7">A fabric-wide configuration activation process failed. An event code 151 is recorded only by the managing switch in the fabric. The event code is intended to help engineering support personnel fault isolate a fabric-wide configuration failures.</td></tr>
<tr><td>Action:</td><td colspan="7">Perform the data collection procedure and return the backup disk to HP support personnel.</td></tr>
<tr><td>Event Data:</td><td colspan="7">Event data are mapped from the software implementation of the FC-SW2 protocol and are typically complicated. Decoding the event data requires engineering support. Event data are as follows:

Bytes 0 - 3 = Managing switch domain ID in internal format (1-31).
Bytes 4 - 7 = Fabric configuration operation that failed.
Bytes 8 - 11 = Fabric configuration step that failed.
Bytes 12 - 15 = Managed switch domain ID in internal format (1-31).
Bytes 16 - 19 = Response command code received from the managed switch.
Bytes 20 - 23 = Response code received from the managed switch.
Bytes 24 - 27 = Reason code received from the managed switch.
Bytes 28 - 31 = Error code received from the managed switch.</td></tr>
<tr><td rowspan="2">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Appliance</td><td colspan="2">Host</td></tr>
<tr><td>EWS Event Log</td><td>System Error LED</td><td>Event Log</td><td>E-Mail</td><td>Call-Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td></td><td>✔</td><td>✔</td><td>✔</td><td></td><td></td><td></td><td></td></tr>
</table>

Power Supply Events (200 through 299)

Table 50: Event Code 200

Message:	Power supply AC voltage failure.						
Severity:	Major.						
Explanation:	Alternating current (AC) input to the indicated power supply is disconnected or AC circuitry in the power supply failed. The second power supply assumes the full operating load for the switch.						
Action:	Ensure the power supply is connected to facility AC power, and verify operation of the facility power source. If the AC voltage does not recover (indicated by event code **203**), replace the failed power supply. Perform the data collection procedure and return the backup disk and failed power supply to Hewlett-Packard support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Table 51: Event Code 201

Message:	Power supply DC voltage failure.						
Severity:	Major.						
Explanation:	Direct current (DC) circuitry in the power supply failed. The second power supply assumes the full operating load for the switch.						
Action:	Replace the failed power supply. Perform the data collection procedure and return the backup disk and failed power supply to Hewlett-Packard support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Table 52: Event Code 202

Message:	Power supply thermal failure.						
Severity:	Major.						
Explanation:	The thermal sensor associated with a power supply indicates an overheat condition that shut down the power supply. The second power supply assumes the full operating load for the switch.						
Action:	Replace the failed power supply. Perform the data collection procedure and return the backup disk and failed power supply to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Table 53: Event Code 203

Message:	Power supply AC voltage recovery.						
Severity:	Informational.						
Explanation:	AC voltage recovered for the power supply. Both power supplies adjust to share operating load for the switch.						
Action:	No action required.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Table 54: Event Code 204

Message:	Power supply DC voltage recovery.
Severity:	Informational.
Explanation:	DC voltage recovered for the power supply. Both power supplies adjust to share operating load for the switch.
Action:	No action required.
Event Data:	No supplementary data included with the event.

Table 54: Event Code 204 (Continued)

Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Table 55: Event Code 206

Message:	Power supply removed.						
Severity:	Informational.						
Explanation:	A power supply was removed while the Switch was powered on and operational. The second power supply assumes the full operating load for the switch.						
Action:	No action required or install an operational power supply.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Table 56: Event Code 207

Message:	Power supply installed.						
Severity:	Informational.						
Explanation:	A redundant power supply was installed with the switch powered on and operational. Both power supplies adjust to share operating load for the switch.						
Action:	No action required.						
Event Data:	No supplementary data included with the event.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Table 57: Event Code 208

Message:	Power supply false shutdown.
Severity:	Major.
Explanation:	Switch operational firmware nearly shut down the indicated power supply as a result of failure or facility power loss or voltage fluctuation.
Action:	Confirm operation of facility power. If subsequent power loss events occur, replace the failed power supply. Perform the data collection procedure and return the backup disk and failed power supply to HP support personnel.

Table 57: Event Code 208 (Continued)

Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Fan Module Events (300 through 399)

Table 58: Event Code 300

Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	One cooling fan (out of four) failed or is rotating at insufficient angular velocity. The remaining fans are operational. The amber LED illuminates at the rear of the failed fan.						
Action:	Replace the indicated fan module.						
Event Data:	The first byte of event data (byte **0**) specifies the failed fan number.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Table 59: Event Code 301

Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	Two cooling fans (out of four) failed or are rotating at insufficient angular velocity. The remaining fans are operational. The amber LED illuminates at the rear of the failed fans.						
Action:	Replace indicated fan modules.						
Event Data:	The first byte of event data (byte **0**) specifies the failed fan numbers.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Table 60: Event Code 302

Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	Three cooling fans (out of four) failed or are rotating at insufficient angular velocity. The remaining fans are operational. The amber LED illuminates at the rear of the failed fans.						
Action:	Replace the indicated fan modules.						
Event Data:	The first byte of event data (byte **0**) specifies the failed fan numbers.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Table 61: Event Code 305

Message:	Cooling fan propeller failed.						
Severity:	Major.						
Explanation:	All four cooling fans failed or are rotating at insufficient angular velocity. The amber LED illuminates at the rear of the failed fan modules.						
Action:	Replace the failed fan modules.						
Event Data:	The first byte of event data (byte **0**) specifies the failed fan numbers.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Table 62: Event Code 310

Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	One cooling fan (out of four) recovered or the fan module was replaced. All fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte **0**) specifies the recovered fan number.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Table 63: Event Code 311

Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	Two cooling fans (out of four) recovered or the fan modules were replaced. All fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte **0**) specifies the recovered fan numbers.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error Indicator	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Table 64: Event Code 312

Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	Three cooling fans (out of four) recovered or the fan modules were replaced. All fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte **0**) specifies the recovered fan numbers.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Table 65: Event Code 315

Message:	Cooling fan propeller recovered.						
Severity:	Informational.						
Explanation:	All four cooling fans recovered or the fan modules were replaced. All fans are operational.						
Action:	No action required.						
Event Data:	The first byte of event data (byte **0**) specifies the recovered fan numbers.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

CTP Card Events (400 through 499)

Table 66: Event Code 400

Message:	Power-up diagnostics failure.						
Severity:	Major.						
Explanation:	Power-on self tests (POSTs) detected a faulty field-replaceable unit (FRU) as indicated by the event data.						
Action:	If a CTP card failure is indicated, replace the switch. If a fan or power supply failure is indicated, replace the power supply assembly. Perform the data collection procedure and return the backup disk and faulty FRU to Hewlett-Packard support personnel.						
Event Data:	Byte **0** = FRU code as follows: **02** = CTP card, **05** = cooling fan, **06** = power supply assembly. Byte **1** = FRU slot number.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Table 67: Event Code 410

Message:	Switch reset.						
Severity:	Informational.						
Explanation:	The switch reset due to system power-up, IML, or manual reset. A software reset can occur automatically after a firmware fault (event code **411**), or be user-initiated. Event data indicates the type of reset.						
Action:	No action required.						
Event Data:	Byte **0** = reset type as follows: **00** = power-on, **02** = IML, **04** = reset.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Table 68: Event Code 411

Message:	Firmware fault.						
Severity:	Major.						
Explanation:	Switch firmware encountered an unexpected condition and dumped operating state information to FLASH memory for retrieval and analysis. The dump file automatically transfers from the switch to the HAFM appliance, where it is stored for later retrieval through the data collection procedure. The switch performs a software reset, during which all attached Fibre Channel devices are momentarily disrupted, log out, and log back in.						
Action:	Perform the data collection procedure and return the backup disk to Hewlett-Packard support personnel.						
Event Data:	Bytes 0 through 3 = fault identifier, least significant byte first.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Table 69: Event Code: 412

Message:	CTP watchdog timer reset.						
Severity:	Informational.						
Explanation:	The hardware watchdog timer expired and caused the CTP card to reset.						
Action:	Perform the data collection procedure and return the backup disk to HP support personnel.						
Event Data:	Byte 0 = reset type as follows: 00 = task switch did not occur within approximately one second, 01 = interrupt servicing blocked for more than approximately one second.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔		✔				

Table 70: Event Code 421

Message:	Firmware download complete.						
Severity:	Informational.						
Explanation:	A switch firmware version was downloaded from the HAFM Appliance or Embedded Web Server. The event data indicates the firmware version in hexadecimal format `xx.yy.zz bbbb`, where `xx` is the release level, `yy` is the maintenance level, `zz` is the interim release level, and `bbbb` is the build ID.						
Action:	No action required.						
Event Data:	Bytes **0** and **1** = release level (`xx`). Byte **2** = always a period. Bytes **3** and **4** = maintenance level (`yy`). Byte **5** = always a period. Bytes **6** and **7** = interim release level (`zz`). Byte **8** = always a space. Bytes **9** through **12** = build ID (`bbbb`).						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Table 71: Event Code 423

Message:	CTP firmware download initiated.						
Severity:	Informational.						
Explanation:	The HAFM appliance initiated download of a new firmware version to the switch.						
Action:	No action required.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Table 72: Event Code 426

Message:	Multiple ECC single-bit errors occurred.						
Severity:	Minor.						
Explanation:	When the SDRAM controller detects an error checking and correction (ECC) error, an interrupt occurs. If an interrupt occurs a certain number of times weekly, a **426** event code is recorded. The number of interrupts is indicated by the event data.						
Action:	No action required. SDRAM is probably malfunctioning intermittently.						
Event Data:	Byte **0** of the event data (equal to **5**, **10**, **15**, or **20**) is recorded. The number of interrupts equals two to the power of the event data. Event data equal to **10** indicates 1,024 ECC error interrupts.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call-Home	Sense Info	Link Incident
	✔		✔				

Table 73: Event Code 430

Message:	Excessive Ethernet transmit errors.
Severity:	Informational.
Explanation:	Transmit error counters for the CTP card Ethernet adapter (sum of all counters) exceeded a threshold. This does not indicate a CTP failure; it indicates a problem with the Ethernet cable, hub, or device on the same Ethernet segment. Event data counters are represented in hexadecimal format with the least significant byte first.
Action:	Verify the Ethernet cable, hub, and other devices are properly connected and operational.
Event Data:	Bytes **0** through **3** = sum of all transmit errors (**total_xmit_error**). Bytes **4** through **7** = frame count where Ethernet adapter does not detect carrier sense at preamble end (**loss_of_CRSs_cnt**). Bytes **8** through **11** = frame count where Ethernet adapter does not detect a collision within 64 bit times at transmission end (**SQE_error_cnt**). Bytes **12** through **15** = frame count where Ethernet adapter detects a collision more than 512 bit times after first preamble bit (**out_of_window_cnt**). Frame not transmitted. Bytes **16** through **19** = frame count where transmission is more than 26 ms (**jabber_cnt**). Frame not transmitted. Bytes **20** through **23** = frame count where Ethernet adapter encounters 16 collisions while attempting to transmit a frame (**16coll_cnt**). Frame not transmitted.

Table 73: Event Code 430 (Continued)

Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Table 74: Event Code 431

Message:	Excessive Ethernet receive errors.						
Severity:	Informational.						
Explanation:	Receive error counters for the CTP card Ethernet adapter (sum of all counters) exceeded a threshold. This does not indicate a CTP failure; it indicates a problem with the Ethernet cable, hub, or device on the same Ethernet segment. Event data counters are represented in hexadecimal format with the least significant byte first.						
Action:	Verify the Ethernet cable, hub, and other devices are properly connected and operational.						
Event Data:	Bytes **0** through **3** = sum of all receive errors (**total_recv_error**). Bytes **4** through **7** = frame count where received frame had from 1 to 7 bits after last received full byte (**dribble_bits_cnt**). CRC error counter updated but frame not processed. Bytes **8** through **11** = frame count where received frame had bad CRC (**CRC_error_cnt**). Frame not processed. Bytes **12** through **15** = frame count received with less than 64 bytes (**runt_cnt**). Broadcast frames count but do not contribute to threshold. Frame not processed. Bytes **16** through **19** = frame count received with more than 1518 bytes (**extra_data_cnt**). Broadcast frames count but do not contribute to threshold. Frame not processed.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Table 75: Event Code 432

Message:	Ethernet adapter reset.						
Severity:	Minor.						
Explanation:	The CTP card Ethernet adapter was reset in response to an internally detected error. A card failure is not indicated. The switch-to-HAFM appliance connection terminates, but automatically recovers after the reset.						
Action:	Perform the data collection procedure and return the backup disk to HP support personnel.						
Event Data:	Bytes **0** through **3** = reason for adapter reset, least significant byte first (**reset_error_type**) **1** = completion notification for timed-out frame transmission.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Table 76: Event Code 433

Message:	Non-recoverable Ethernet fault.						
Severity:	Major.						
Explanation:	A non-recoverable Ethernet interface failure was detected and the LAN connection to the HAFM appliance or Internet was terminated. No failure information or event codes are reported outside the switch. Although Fibre Channel port functionality is not affected, the switch cannot be monitored or configured.						
Action:	Replace the switch.						
Event Data:	Byte **0** = LAN error type as follows: **01** = hard failure, **04** = registered fault. Byte **1** = LAN error subtype (internally defined). Byte **2** = LAN fault identifier (internally defined).						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Table 77: Event Code 440

Message:	Embedded port hardware failed.						
Severity:	Major.						
Explanation:	The embedded port hardware detected a fatal CTP error.						
Action:	Replace the switch.						
Event Data:	Byte **0** = CTP slot position (**00**). Byte **1** = engineering reason code Bytes **4** through **7** = elapsed millisecond tick count.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Table 78: Event Code 442

Message:	Embedded port anomaly detected.						
Severity:	Informational.						
Explanation:	The switch detected a deviation in the normal operating mode or status of the embedded port.						
Action:	No action required. An additional event code is generated if this incident exceeds an error threshold or results in a port failure.						
Event Data:	Byte **0** = port number. Byte **1** = engineering reason code.port. Bytes **4** through **7** = elapsed millisecond tick count. Bytes **8** and **9** = high-availability error callout #1. Bytes **10** and **11** = high-availability error callout #2. Byte **12** = detecting port. Byte **13** = connected port. Bytes **16** and **17** = high-availability error callout #3. Bytes **18** and **19** = high-availability error callout #4.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Table 79: Event Code 445

<table>
<tr><td>Message:</td><td colspan="7">ASIC detected a system anomaly.</td></tr>
<tr><td>Severity:</td><td colspan="7">Informational.</td></tr>
<tr><td>Explanation:</td><td colspan="7">The application-specific integrated chip (ASIC) detected a deviation in the normal operating mode or operating status of the switch.</td></tr>
<tr><td>Action:</td><td colspan="7">No action required. An additional event code is generated if this incident exceeds an error threshold that results in a system event.</td></tr>
<tr><td>Event Data:</td><td colspan="7">Byte 0 = port number.
Byte 1 = engineering reason code.port.
Bytes 4 through 7 = elapsed millisecond tick count.
Bytes 8 and 9 = high-availability error callout #1.
Bytes 10 and 11 = high-availability error callout #2.
Byte 12 = detecting port.
Byte 13 = connected port.
Bytes 16 and 17 = high-availability error callout #3.
Bytes 18 and 19 = high-availability error callout #4.</td></tr>
<tr><td rowspan="3">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Appliance</td><td colspan="2">Host</td></tr>
<tr><td>EWS Event Log</td><td>System Error LED</td><td>Event Log</td><td>E-Mail</td><td>Call Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td>✔</td><td></td><td>✔</td><td></td><td></td><td></td><td></td></tr>
</table>

Table 80: Event Code 453

Message:	New feature key installed.						
Severity:	Informational.						
Explanation:	This event occurs when a new feature key is installed from the HAFM appliance or EWS interface. The switch performs an IPL when the feature key is enabled. Event data indicates which feature or features are installed.						
Action:	No action required.						
Event Data:	Byte **0** = feature description as follows: **00** through **04** = Flexport, **06** = open-system management server. Byte **1** = feature description as follows: **06** = SANtegrity Binding, **07** = Open Trunking						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Table 81: Event Code 460

Message:	Management request out of range.						
Severity:	Informational						
Explanation:	This event occurs when requests passed from the managing tool (generally HAFM) to the switch do not meet data boundary specifications. This event is most likely to be triggered if a user attempt to activate a zone set that is larger than the maximum defined zone set size.						
Action:	The switch found request data from the management tool to be larger or smaller than expected. The connection to the management tool will be temporarily lost. After the link is re-established, verify that all information changed in the managing tool is within the specified ranges. For example, verify that the zones and zone members in a zone set fall within the limits stated in the user manual. Try sending the request again.						
Event Data:	None						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Port Events (500 through 599)

Table 82: Event Code 506

<table>
<tr><td>Message:</td><td colspan="7">Fibre Channel port failure.</td></tr>
<tr><td>Severity:</td><td colspan="7">Major.</td></tr>
<tr><td>Explanation:</td><td colspan="7">A Fibre channel port failed. The amber LED corresponding to the port illuminates to indicate the failure. Other ports remain operational if their LEDs are extinguished.</td></tr>
<tr><td>Action:</td><td colspan="7">Perform the data collection procedure and return the backup disk to Hewlett-Packard support personnel.
Perform a switch reset. If the problem persists, replace the switch.</td></tr>
<tr><td>Event Data:</td><td colspan="7">Byte 0 = port number (00 through 31).
Byte 1 = engineering reason code.
Bytes 4 through 7 = elapsed millisecond tick count.
Bytes 8 through 11 = reason code specific.
Byte 16 = connector type.
Bytes 17 and 18 = transmitter technology.
Byte 19 = distance capabilities.
Byte 20 = supported transmission media.
Byte 21 and 22 = speed capability and configuration.</td></tr>
<tr><td rowspan="3">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Appliance</td><td colspan="2">Host</td></tr>
<tr><td>EWS Event Log</td><td>System Error LED</td><td>Event Log</td><td>E-Mail</td><td>Call Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td>✔</td><td>✔</td><td>✔</td><td>✔</td><td>✔</td><td>✔</td><td></td></tr>
</table>

Table 83: Event Code 507

Message:	Loopback diagnostics port failure.						
Severity:	Informational.						
Explanation:	A loopback diagnostic test detected a Fibre Channel port failure.						
Action:	No action required. An event code **506** is generated if this diagnostic failure results in a hard port failure.						
Event Data:	Byte **0** = port number (**00** through **31**). Byte **1** = engineering reason code. Bytes **4** through **7** = elapsed millisecond tick count. Bytes **8** through **11** = reason code specific. Byte **12** = test type.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Table 84: Event Code 508

Message:	Fibre Channel port anomaly detected.
Severity:	Informational.
Explanation:	The CTP detected a deviation in the normal operating mode or status of the indicated Fibre Channel port.
Action:	No action required. An event code **506** is generated if this anomaly results in a hard port failure.
Event Data:	Byte **0** = port number (**00** through **31**). Byte **1** = anomaly reason code. Bytes **4** through **7** = elapsed millisecond tick count. Bytes **8** and **9** = high-availability error callout #1. Bytes **10** and **11** = high-availability error callout #2. Byte **12** = detecting port. Byte **13** = connected port. Bytes **16** and **17** = high-availability error callout #3. Bytes **18** and **19** = high-availability error callout #4.

Table 84: Event Code 508 (Continued)

Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Table 85: Event Code 510

Message:	SFP optical transceiver hot-insertion initiated.						
Severity:	Informational.						
Explanation:	Installation of a small form factor pluggable (SFP) optical transceiver was initiated with the switch powered on and operational. The event indicates that operational firmware detected the presence of the transceiver.						
Action:	No action required.						
Event Data:	Byte **0** = port number (**00** through **31**). Bytes **4** through **7** = elapsed millisecond tick count.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Table 86: Event Code 512

Message:	SFP optical transceiver nonfatal error.						
Severity:	Minor.						
Explanation:	Switch firmware detected an SFP optical transceiver non-fatal error.						
Action:	Replace the failed transceiver with a functional transceiver of the same type.						
Event Data:	Byte **0** = port number (**00** through **31**). Byte **1** = engineering reason code. Bytes **4** through **7** = elapsed millisecond tick count.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Table 87: Event Code 513

Message:	SFP optical transceiver hot-removal completed.						
Severity:	Informational.						
Explanation:	An SFP optical transceiver was removed while the switch was powered on and operational.						
Action:	No action required.						
Event Data:	Byte **0** = port number (**00** through **31**). Bytes **4** through **7** = elapsed millisecond tick count.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Table 88: Event Code 514

Message:	SFP optical transceiver failure.						
Severity:	Major.						
Explanation:	An SFP optical transceiver failed. The amber LED corresponding to the port illuminates to indicate the failure. Other ports remain operational if their LEDs are extinguished.						
Action:	Replace the failed transceiver with a functional transceiver of the same type.						
Event Data:	Byte **0** = port number (**00** through **31**). Byte **1** = engineering reason code. Bytes **4** through **7** = elapsed millisecond tick count.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Table 89: Event Code 581

Message:	Implicit incident.						
Severity:	Major.						
Explanation:	An attached open systems interconnection (OSI) server recognized a condition caused by an event that occurred at the server. The event caused an implicit Fibre Channel link incident.						
Action:	A link incident record (LIR) is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to "MAP 0000: Start MAP" on page 29 to perform fault isolation.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
			✔				✔

Table 90: Event Code 582

Message:	Bit error threshold exceeded.						
Severity:	Major.						
Explanation:	An attached OSI server determined the number of code violation errors recognized exceeded the bit error threshold.						
Action:	An LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to "MAP 0000: Start MAP" on page 29 to perform fault isolation.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
			✔				✔

Table 91: Event Code 583

Message:	Loss of signal or loss of synchronization.						
Severity:	Major.						
Explanation:	An attached OSI server recognized a loss-of-signal condition or a loss-of-synchronization condition that persisted for more than the specified receiver-transmitter timeout value (R_T_TOV).						
Action:	An LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to "MAP 0000: Start MAP" on page 29 to perform fault isolation.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
			✔				✔

Table 92: Event Code 584

Message:	Not operational primitive sequence received.						
Severity:	Major.						
Explanation:	An attached OSI server received a not-operational primitive sequence (NOS).						
Action:	An LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to "MAP 0000: Start MAP" on page 29 to perform fault isolation.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
			✔				✔

Table 93: Event Code 585

Message:	Primitive sequence timeout.						
Severity:	Major.						
Explanation:	An attached OSI server recognized either a link reset (LR) protocol timeout or a timeout while waiting for the appropriate response (while in a NOS receive state and after NOS was not longer recognized).						
Action:	An LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to "MAP 0000: Start MAP" on page 29 to perform fault isolation.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
			✔				✔

Table 94: Event Code 586

Message:	Invalid primitive sequence received for current link state.						
Severity:	Major.						
Explanation:	An attached OSI server recognized either a link reset (LR) or a link-reset response (LRR) sequence while in the wait-for-online sequence (OLS) state.						
Action:	An LIR is generated and sent to the attached server using the reporting procedure defined in T11/99-017v0 (OSI). If fault isolation at the server does not detect a failure, the problem may be due to a port failure. Go to "MAP 0000: Start MAP" on page 29 to perform fault isolation.						
Event Data:	Refer to the T11/99-017v0 document for the specific link incident record format.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
			✔				✔

SBAR Events (600 through 699)

In the Edge Switch 2/32, the SBAR is not a separate assembly, therefore not a FRU. It is an integral part of the switch's main circuit board. SBAR failure requires replacement of the entire switch.

Table 95: Event Code 602

<table>
<tr><td>Message:</td><td colspan="7">SBAR module anomaly detected.</td></tr>
<tr><td>Severity:</td><td colspan="7">Informational.</td></tr>
<tr><td>Explanation:</td><td colspan="7">Indicates that the control processor has detected a deviation in the normal operating mode or operating status of the indicated SBAR module.</td></tr>
<tr><td>Action:</td><td colspan="7">No action required. There will be an additional event generated (604) if this event results in an SBAR logic failure.</td></tr>
<tr><td>Event Data:</td><td colspan="7">Byte 0 = Slot position.
Byte 1 = Anomaly reason code (See following chart).
Bytes 4–7 = Elapsed millisecond tick count.
Bytes 8–9 = High Availability error callout #1.
Bytes 10–11 = High Availability error callout #2.
Byte 12 = Detecting port.
Byte 13 = Connected port.
Byte 14 = Participating SBAR.
Bytes 16–17 = High Availability error callout #3.
Bytes 18–19 = High Availability error callout #4.</td></tr>
<tr><td rowspan="2">Distribution:</td><td colspan="2">Switch</td><td colspan="3">HAFM Appliance</td><td colspan="2">Host</td></tr>
<tr><td>Non-volatile System Event Log</td><td>System Error Indicator</td><td>Event Log</td><td>E-Mail</td><td>Call Home</td><td>Sense Info</td><td>Link Incident</td></tr>
<tr><td></td><td>✔</td><td></td><td>✔</td><td></td><td></td><td></td><td></td></tr>
</table>

Table 96: Event Code 604

Message:	SBAR module failure.						
Severity:	Major.						
Explanation:	A failure criteria associated with the serial crossbar hardware module has been met.						
Action:	Perform the data collection procedure for the switch using HAFM, save the data file to the HAFM appliance backup drive, and return the backup disk to HP support personnel for analysis.						
Event Data:	Byte **0** = Slot position. Byte **1** = Reason code: 00 = Operator requested with debug command. 02 = Initialization failure. 03 = Hot plug/power up diagnostics failure acknowledgement. 04 = Communications with hardware is irregular or nonexistent. 05 = Read of module ID failed. 06 = High availability statistical error threshold reached. 07 = Communication with hardware is irregular or nonexistent. Bytes **4–7** = Elapsed millisecond tick counter. Bytes **8–11** = Reason code specific data.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error Indicator	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Table 97: Event Code 605

Message:	SBAR module revision not supported.
Severity:	Minor.
Explanation:	The specified SBAR module is not recognized by the existing firmware. The SBAR module will appear uninstalled to system software.
Action:	Ensure that the switch model supports the operating firmware. If the firmware supports the model, perform the data collection procedure for the switch using HAFM. If the problem persists following a system power-on reset, replace the switch and return the switch and the backup disk to HP support personnel for analysis and repair.

Table 97: Event Code 605

Event Data:	Byte **0** = Slot position. Bytes **4–7** = Elapsed millisecond tick counter. Bytes **8–9**: = Detected Module identifier.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error Indicator	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔		✔				

Thermal Events (800 through 899)

Table 98: Event Code 805

Message:	High-temperature warning (SBAR module thermal sensor).						
Severity:	Major.						
Explanation:	The thermal sensor associated with the SBAR module has detected that the “warm” temperature threshold level has been surpassed.						
Action:	Perform the data collection procedure for this switch using HAFM, Save the data file to the HAFM backup drive, and return the backup disk to HP support personnel for analysis. Perform a system power-on reset. If the problem persists, replace the switch.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error Indicator	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Table 99: Event Code 806

Message:	Critically hot temperature warning (SBAR module thermal sensor).						
Severity:	Major.						
Explanation:	The thermal sensor associated with the SBAR module has detected that the “hot” temperature threshold level has been surpassed.						
Action:	Perform the data collection procedure for this switch using HAFM, Save the data file to the HAFM backup drive, and return the backup disk to HP support personnel for analysis. Perform a system power-on reset. If the problem persists, replace the switch.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error Indicator	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Table 100: Event Code 807

Message:	SBAR module shutdown due to thermal violation.						
Severity:	Major.						
Explanation:	The SBAR Module has been marked failed and power has been removed from the module due to excessive heat. This event follows an indication that the SBAR module "hot" threshold level has been surpassed (event 806).						
Action:	Perform the data collection procedure for this switch using HAFM, Save the data file to the HAFM backup drive, and return the backup disk to HP support personnel for analysis. Perform a system power-on reset. If the problem persists, replace the switch.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error Indicator	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Table 101: Event Code 810

Message:	High temperature warning (CTP card thermal sensor).						
Severity:	Major.						
Explanation:	The thermal sensor associated with a CTP card indicates the warm temperature threshold was reached or exceeded.						
Action:	Replace the failed switch. Perform the data collection procedure and return the backup disk and faulty switch to Hewlett-Packard support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error Indicator	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Table 102: Event Code 811

Message:	Critically hot temperature warning (CTP card thermal sensor).						
Severity:	Major.						
Explanation:	The thermal sensor associated with a CTP card indicates the hot temperature threshold was reached or exceeded.						
Action:	Replace the failed switch. Perform the data collection procedure and return the backup disk and faulty switch to Hewlett-Packard support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Table 103: Event Code 812

Message:	CTP card shutdown due to thermal violation.						
Severity:	Major.						
Explanation:	A CTP failed and was powered off because of excessive heat. This event follows an indication that the hot temperature threshold was reached or exceeded (event code **811**).						
Action:	Replace the failed switch. Perform the data collection procedure and return the backup disk and faulty switch to HP support personnel.						
Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

Table 104: Event Code 850

Message:	System shutdown due to CTP card thermal violations.
Severity:	Severe.
Explanation:	The switch powered off because of excessive thermal violations on the CTP card.
Action:	Replace the failed switch. Perform the data collection procedure and return the backup disk and faulty switch to HP support personnel.

Table 104: Event Code 850

Event Data:	No supplementary data included with this event.						
Distribution:	Switch		HAFM Appliance			Host	
	EWS Event Log	System Error LED	Event Log	E-Mail	Call Home	Sense Info	Link Incident
	✔	✔	✔	✔	✔	✔	

index

F

N

O

P

R

S

T

U

V

W